Exhibit 4

Combating Trafficking in Counterfeit and Pirated Goods

Report to the President of the United States

January 24, 2020

Homeland Security

Office of Strategy, Policy & Plans

Table of Contents

Foreword/Message from the Acting Secretary of Homeland Security

The rapid growth of e-commerce has revolutionized the way goods are bought and sold, allowing for counterfeit and pirated goods to flood our borders and penetrate our communities and homes. Illicit goods trafficked to American consumers by e-commerce platforms and online third-party marketplaces threaten public health and safety, as well as national security. This illicit activity impacts American innovation and erodes the competitiveness of U.S. manufacturers and workers.

Consumers must be confident in the safety, quality, and authenticity of the products they purchase online. DHS is committed to combating counterfeiters and pirates with the help of our U.S. Government partners and private sector stakeholders - who are critical to helping secure supply chains to stem the tide of counterfeit and pirated goods.

"Combating Trafficking in Counterfeit and Pirated Goods," has been prepared by the U.S. Department of Homeland Security's Office of Strategy, Policy, and Plans. The report uses available data, substantial public input, and other information to develop a deeper understanding of how e-commerce platforms, online third-party marketplaces, and other third-party intermediaries facilitate the importation and sale of massive amounts of counterfeit and pirated goods. The report identifies appropriate administrative, statutory, regulatory, and other actions, including enhanced enforcement measures, modernization of legal and liability frameworks, and best practices for private sector stakeholders. These strong actions can be implemented swiftly to substantially reduce trafficking in counterfeit and pirated goods while promoting a safer America.

This report was prepared pursuant to President Donald J. Trump's April 3, 2019, *Memorandum on Combating Trafficking in Counterfeit and Pirated Goods*. The President's historic memorandum provides a much warranted and long overdue call to action in the U.S. Government's fight against a massive form of illicit trade that is inflicting significant harm on American consumers and businesses. This illicit trade must be stopped in its tracks.

This report was prepared in coordination with the Secretaries of Commerce and State, the Attorney General, the Office of Management and Budget, the Intellectual Property Enforcement Coordinator, the United States Trade Representative, the Assistant to the President for Economic Policy, the Assistant to the President for Trade and Manufacturing Policy, and with other partners in the U.S. Government. The report also benefitted from extensive engagement with the private sector.

Sincerely,

Chad Wolf
Acting Secretary,
U.S. Department of Homeland Security

1. Executive Summary

The President's April 3, 2019, *Memorandum on Combating Trafficking in Counterfeit and Pirated Goods* calls prompt attention to illicit trade that erodes U.S. economic competitiveness and catalyzes compounding threats to national security and public safety.

Counterfeiting is no longer confined to street-corners and flea markets. The problem has intensified to staggering levels, as shown by a recent Organisation for Economic Cooperation and Development (OECD) report, which details a 154 percent increase in counterfeits traded internationally — from $200 billion in 2005 to $509 billion in 2016. Similar information collected by the U.S. Department of Homeland Security (DHS) between 2000 and 2018 shows that seizures of infringing goods at U.S. borders have increased 10-fold, from 3,244 seizures per year to 33,810.

Relevant to the President's inquiry into the linkages between e-commerce and counterfeiting, OECD reports that "E-commerce platforms represent ideal storefronts for counterfeits and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers."[1] Similarly, the U.S. Government Accountability Office (GAO) found that e-commerce has contributed to a shift in the sale of counterfeit goods in the United States, with consumers increasingly purchasing goods online and counterfeiters producing a wider variety of goods that may be sold on websites alongside authentic products.

Respondents to the July 10, 2019, Federal Register Notice issued by the Department of Commerce echoed these observations.[2] Perhaps most notably, the International Anti-Counterfeiting Coalition (IACC) reports that the trafficking of counterfeit and pirated goods in e-commerce is a top priority for every sector of its membership — comprised of more than 200 corporations, including many of the world's best-known brands in the apparel, automotive, electronics, entertainment, luxury goods, pharmaceutical, personal care and software sectors. The IACC submission goes on to say:

> *Across every sector of the IACC's membership, the need to address the trafficking of counterfeit and pirated goods in e-commerce has been cited as a top priority. The vast amounts of resources our members must dedicate to ensuring the safety and vitality of the online marketplace, bears out the truth of the issue highlighted by Peter Navarro, Assistant to the President for Trade and Manufacturing Policy, in his April 3, 2019 Op-Ed piece in The Wall Street Journal - that the sale of counterfeit brand-name goods presents a pervasive and ever-growing threat in the online space. One IACC member reported making*

[1] OECD (2018), *Governance Frameworks to Counter Illicit Trade*, Illicit Trade, OECD Publishing, Paris, https://doi.org/10.1787/9789264291652-en.

[2] Under Federal Register Notice (84 FR 32861), the Department of Commerce sought "comments from intellectual property rights holders, online third-party marketplaces and other third-party intermediaries, and other private-sector stakeholders on the state of counterfeit and pirated goods trafficking through online third-party marketplaces and recommendations for curbing the trafficking in such counterfeit and pirated goods."

> *hundreds of investigative online test purchases over the past year, with a nearly 80% successfully resulting in the receipt of a counterfeit item.*[3]

The scale of counterfeit activity online is evidenced as well by the significant efforts e-commerce platforms themselves have had to undertake. A major e-commerce platform reports that its proactive efforts prevented over 1 million suspected bad actors from publishing a single product for sale through its platform and blocked over 3 billion suspected counterfeit listings from being published to their marketplace. Despite efforts such as these, private sector actions have not been sufficient to prevent the importation and sale of a wide variety and large volume of counterfeit and pirated goods to the American public.

The projected growth of e-commerce fuels mounting fears that the scale of the problem will only increase, especially under a business-as-usual scenario. Consequently, an effective and meaningful response to the President's memorandum is a matter of national import.

Actions to be Taken by DHS and the U.S. Government

Despite public and private efforts to-date, the online availability of counterfeit and pirated goods continues to increase. Strong government action is necessary to fundamentally realign incentive structures and thereby encourage the private sector to increase self-policing efforts and focus more innovation and expertise on this vital problem. Therefore, DHS will immediately undertake the following actions and make recommendations for other departments and agencies to combat the trafficking of counterfeit and pirated goods.

Immediate Actions by DHS and Recommendations for the U.S. Government
1. Ensure Entities with Financial Interests in Imports Bear Responsibility
2. Increase Scrutiny of Section 321 Environment
3. Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Posts
4. Apply Civil Fines, Penalties and Injunctive Actions for Violative Imported Products
5. Leverage Advance Electronic Data for Mail Mode
6. Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION) Plan
7. Analyze Enforcement Resources
8. Create Modernized E-Commerce Enforcement Framework
9. Assess Contributory Trademark Infringement Liability for Platforms
10. Re-Examine the Legal Framework Surrounding Non-Resident Importers
11. Establish a National Consumer Awareness Campaign

[3] International Anti-Counterfeiting Coalition's comments made on the Department of Commerce, International Trade Administration, Office of Intellectual Property Rights', Report on the State of Counterfeit and Pirated Goods Trafficking Recommendations, 29 July 2019. Posted on 6 August 2019. https://www.regulations.gov/document?D=DOC-2019-0003-0072

Best Practices for E-Commerce Platforms and Third-Party Marketplaces

Government action alone is not enough to bring about the needed paradigm shift and ultimately stem the tide of counterfeit and pirated goods. All relevant private-sector stakeholders have critical roles to play and must adopt identified best practices, while redoubling efforts to police their own businesses and supply chains.

While the U.S. brick-and-mortar retail store economy has a well-developed regime for licensing, monitoring, and otherwise ensuring the protections of intellectual property rights (IPR), a comparable regime is largely non-existent for international e-commerce sellers. The following table catalogs a set of high priority "best practices" that shall be communicated to all relevant private sector stakeholders by the National Intellectual Property Rights Coordination Center. It shall be the Center's duty to monitor and report on the adoption of these best practices within the scope of the legal authority of DHS and the Federal government.

Best Practices for E-Commerce Platforms and Third-Party Marketplaces
1. Comprehensive "Terms of Service" Agreements
2. Significantly Enhanced Vetting of Third-Party Sellers
3. Limitations on High Risk Products
4. Rapid Notice and Takedown Procedures
5. Enhanced Post-Discovery Actions
6. Indemnity Requirements for Foreign Sellers
7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests for Information (RFI)
8. Pre-Sale Identification of Third-Party Sellers
9. Establish Marketplace Seller ID
10. Clearly Identifiable Country of Origin Disclosures

Foremost among these best practices is the idea that e-commerce platforms, online third-party marketplaces, and other third-party intermediaries such as customs brokers and express consignment carriers must take a more active role in monitoring, detecting, and preventing trafficking in counterfeit and pirated goods.

2. Introduction

> *E-commerce platforms represent ideal storefronts for counterfeits…and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers.*
>
> **- Organisation for Economic Cooperation and Development**[4]

The rapid growth of e-commerce platforms, further catalyzed by third-party online marketplaces connected to the platforms, has revolutionized the way products are bought and sold. "Online third-party marketplace" means any web-based platform that includes features primarily designed for arranging the sale, purchase, payment, or shipping of goods, or that enables sellers not directly affiliated with an operator of such platforms to sell physical goods to consumers located in the United States.

In the United States, e-commerce year-over-year retail sales grew by 13.3 percent in the second quarter of 2019 while total retail sales increased by only 3.2 percent as brick-and-mortar retail continued its relative decline.[5] For example, Amazon reports third-party sales on its marketplace grew from $100 million in 1999 to $160 *billion* in 2018.[6] In 2018 alone, Walmart experienced an e-commerce sales increase of 40 percent.[7]

Counterfeits threaten national security and public safety directly when introduced into government and critical infrastructure supply chains, and indirectly if used to generate revenue for transnational criminal organizations. Counterfeits also pose risks to human health and safety, erode U.S. economic competitiveness and diminish the reputations and trustworthiness of U.S. products and producers. Across all sectors of the economy, counterfeit goods unfairly compete with legitimate products and reduce the incentives to innovate, both in the United States and abroad.

While the expansion of e-commerce has led to greater trade facilitation, its overall growth—especially the growth of certain related business models—has facilitated online trafficking in counterfeit and pirated goods. American consumers shopping on e-commerce platforms and online third-party marketplaces now face a significant risk of purchasing counterfeit or pirated goods. This risk continues to rise despite current efforts across e-commerce supply chains to reduce such trafficking.

---

[4] OECD (2018), *Governance Frameworks to Counter Illicit Trade*, Illicit Trade, OECD Publishing, Paris, https://doi.org/10.1787/9789264291652-en.

[5] Department of Commerce, U.S. Census Bureau, Economic Indicators Division, "Quarterly Retail E-Commerce Sales 2nd Quarter 2019," 19 August 2019. https://www2.census.gov/retail/releases/historical/ecomm/19q2.pdf

[6] Jeff Bezos, "2018 Letter to Shareholders," *The Amazon Blog*. 11 April 2019. https://blog.aboutamazon.com/company-news/2018-letter-to-shareholders

[7] Note: Walmart does not separate out the percentage of third-party vendor sales. More information can be found, *here*, Jaiswal, Abhishek, "Getting Started Selling on Walmart in 2019: An Insider's Guide to Success," *BigCommerce*. https://www.bigcommerce.com/blog/selling-on-walmart-marketplace/#millennials-are-the-drivers-of-legacy-brand-change-including-walmart. *See also*, "Walmart Marketplace: Frequently Asked Questions," *Walmart.* https://marketplace.walmart.com/resources/#1525808821038-8edf332b-5ba2.

The OECD reports international trade in counterfeit and pirated goods amounted to as much as $509 billion in 2016. This represents a 3.3 percent increase from 2013 as a proportion of world trade. From 2003[8] through 2018, seizures of infringing goods by the U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) increased from 6,500 to 33,810 while the domestic value of seized merchandise — as measured by manufacturer's suggested retail price of the legitimate good (MSRP) — increased from $94 million in 2003 to $1.4 billion in 2018.[9]

The rise in consumer use of third-party marketplaces significantly increases the risks and uncertainty for U.S. producers when creating new products. It is no longer enough for a small business to develop a product with significant local consumer demand and then use that revenue to grow the business regionally, nationally, and internationally with the brand protection efforts expanding in step. Instead, with the international scope of e-commerce platforms, once a small business exposes itself to the benefits of placing products online — which creates a geographic scope far greater than its more limited brand protection efforts can handle — it begins to face increased foreign infringement threat.

Moreover, as costs to enter the online market have come down, such market entry is happening earlier and earlier in the product cycle, further enhancing risk. If a new product is a success, counterfeiters will attempt, often immediately, to outcompete the original seller with lower-cost counterfeit and pirated versions while avoiding the initial investment into research and design.

In other words, on these platforms, the counterfeit and pirated goods compete unfairly and fraudulently against the genuine items. While counterfeit and pirated goods have been sold for years on street corners, alleys, and from the trunks of cars, these illicit goods are now marketed to consumers in their homes through increasingly mainstream e-commerce platforms and third party online marketplaces that convey an air of legitimacy.

With the rise of e-commerce, the problem of counterfeit trafficking has intensified. The OECD documents a 154 percent increase in counterfeits traded internationally, from $200 billion in 2005 to $509 billion in 2016.[10] Data collected by CBP between 2000 and 2018 shows that seizures of infringing goods at U.S. borders, much of it trafficked through e-commerce, has increased ten-fold. Over 85 percent of the contraband seized by CBP arrived from China and Hong Kong. These high rates of seizures are consistent with a key OECD finding.

> *Counterfeit and pirated products come from many economies, with China appearing as the single largest producing market. These illegal products are frequently found in a range of industries, from luxury items (e.g. fashion apparel or deluxe watches), via intermediary products (such as machines, spare parts or*

[8] https://www.cbp.gov/sites/default/files/documents/FY2003%20IPR%20Seizure%20Statistics_0.pdf.
[9] https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR_Annual-Report-FY-2018.pdf
[10] OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris. https://www.oecd-ilibrary.org/docserver/9789264252653-en.pdf?expires=1576509401&id=id&accname=id5723&checksum=576BF246D4E50234EAF5E8EDF7F08147

chemicals) to consumer goods that have an impact on personal health and safety (such as pharmaceuticals, food and drink, medical equipment, or toys).[11]

Operation Mega Flex

In 2019, in response to the alarmingly high rates of contraband uncovered by DHS and a request from the White House Office of Trade and Manufacturing Policy (OTMP), CBP initiated Operation Mega Flex. This operation uses enhanced inspection and monitoring efforts to identify high-risk violators that are shipping and receiving illicit contraband through international mail facilities and express consignment hubs.

The periodic "blitz operations" conducted under the auspices of Operation Mega Flex examine thousands of parcels from China and Hong Kong and carefully catalog the range of contraband seized. To date, such operations have included visits to seven of CBP's international mail facilities and four express consignment hubs and the completion of over 20,000 additional inspections. The following table summarizes the findings of three Mega Flex blitzes conducted between July and September of 2019.

Results of Operation Mega Flex (2019)				
	Blitz I *July 16 & 17*	Blitz II *August 21*	Blitz III *September 18*	Total
Inspections	9,705	5,757	5,399	20,861
Discrepancies	1,145	1,010	735	2,890
Discrepancy Rate	11.8%	17.5%	13.6%	13.9%
Counterfeits	212	467	382	1,061
Counterfeit Rate	2.2%	8.1%	7.1%	5.1%

Source: U.S. Customs and Border Protection

Among the discrepancies uncovered by Operation Mega Flex were 1,061 shipments of counterfeit products. These counterfeits range from fake name brand items, like Louis Vuitton bags to sports equipment made with faulty parts. Other contraband included drug paraphernalia, deadly opioids, and counterfeit drivers' licenses.[12] In all, counterfeits constituted more than one of every three discrepancies uncovered by inspectors.[13]

---

[11] OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris. https://www.oecd-ilibrary.org/docserver/9789264252653-en.pdf?expires=1576509401&id=id&accname=id5723&checksum=576BF246D4E50234EAF5E8EDF7F08147

[12] Oren Fliegelman, "Made in China: Fake IDs," *The New York Times.* 6 February 2015. https://www.nytimes.com/2015/02/08/education/edlife/fake-ids-or-why-would-a-student-order-a-tea-set.html

[13] Among the near 3,000 discrepancies, 20% of them were agricultural violations, such as bad meat, fruit, or produce, unsafe for the American consumer. These agricultural discrepancies are dangerous to the United States because they may contain diseases or pests that can greatly impact agriculture. For example, on October 16, 2018, CBP seized nearly 900 pounds of mitten crabs from an incoming Chinese freight. In Asia, mitten crabs are considered a seasonal delicacy; however, they have a disastrous impact on other global habitats and are labeled as an invasive species. See, Department of Homeland Security, U.S. Customs and Border Protection, "CBP Prevents Smuggling of Nearly 900 Pounds of Invasive Mitten Crabs," 31 October 2018. https://www.cbp.gov/newsroom/national-media-release/cbp-prevents-smuggling-nearly-900-pounds-invasive-mitten-crabs.

Authorities also seized 174 controlled or prohibited substances, including: recreational drugs like LSD, cocaine, DMT, ecstasy, marijuana, mushrooms, and poppy pods as well as steroids and highly addictive painkillers like Tramadol.

It is not just a rise in the volume of counterfeits we are witnessing. GAO notes that counterfeiters are increasingly producing a "wider variety of goods that may be sold on websites alongside authentic products."[14]

DHS finds the current state of e-commerce to be an intolerable and dangerous situation that must be addressed firmly and swiftly by strong actions within the Department and across other relevant agencies of the U.S. Government (USG). These include: The Federal Bureau of Investigation and the Department of Justice, the Department of Commerce, and the Department of the Treasury. This report provides a blueprint for swift and constructive changes and sets forth several actions for immediate implementation.

3. Overview of Counterfeit and Pirated Goods Trafficking

While most e-commerce transactions involve legitimate sellers and products, far too many involve the trafficking of counterfeit and pirated goods and expose legitimate businesses and consumers to substantial risks. This is a global phenomenon; the OECD reports international trade in counterfeit and pirated goods amounted to as much as half a trillion dollars in 2016.[15]

Key Drivers of Counterfeiting and Piracy in E-Commerce

Historically, many counterfeits were distributed through swap meets and individual sellers located on street corners. Today, counterfeits are being trafficked through vast e-commerce supply chains in concert with marketing, sales, and distribution networks. The ability of e-commerce platforms to aggregate information and reduce transportation and search costs for consumers provides a big advantage over brick-and-mortar retailers. Because of this, sellers on digital platforms have consumer visibility well beyond the seller's natural geographical sales area.

Selling counterfeit and pirated goods through e-commerce is a highly profitable activity: production costs are low, millions of potential customers are available online, transactions are convenient, and listing on well-branded e-commerce platforms provides an air of legitimacy.

Other discrepancies found by CBP in the blitz operations included 13 weapon modifications and gun parts, 3 occurrences of drug paraphernalia, and 3 pill presses. For full summary of findings, see, Department of Homeland Security, U.S. Customs and Border Protection, Operation Mega Flex I, II and III Summaries, 2019.

[14]U.S. Government Accountability Office Report to the Chairman, Committee on Finance, U.S. Senate: *Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market*, GAO-18-216, Washington, DC: Government Accountability Office, January 2018. https://www.gao.gov/assets/690/689713.pdf

[15]See OECD, Trends in Trade in Counterfeit and Pirated Goods (March 2019), available at https://www.oecd.org/governance/risk/trends-in-trade-in-counterfeit-and-pirated-goods-g2g9f533-en.htm

[15]See Parker et al. 2016

When sellers of illicit goods are in another country, they are largely outside the jurisdiction for criminal prosecution or civil liability from U.S. law enforcement and private parties.

The Role of Online Third-Party Marketplaces

Third-party online marketplaces can quickly and easily establish attractive "store-fronts" to compete with legitimate businesses. On some platforms, little identifying information is necessary to begin selling.

A counterfeiter seeking to distribute fake products will typically set up one or more accounts on online third-party marketplaces. The ability to rapidly proliferate third-party online marketplaces greatly complicates enforcement efforts, especially for intellectual property rights holders. Rapid proliferation also allows counterfeiters to hop from one profile to the next even if the original site is taken down or blocked. On these sites, online counterfeiters can misrepresent products by posting pictures of authentic goods while simultaneously selling and shipping counterfeit versions.

Counterfeiters have taken full advantage of the aura of authenticity and trust that online platforms provide. While e-commerce has supported the launch of thousands of legitimate businesses, their models have also enabled counterfeiters to easily establish attractive "store-fronts" to compete with legitimate businesses.

Platforms use their third-party marketplace functions to leverage "two-sided" network effects to increase profitability for the platform by adding both more sellers and more buyers. Because sellers benefit with each additional buyer using the platform (more consumers to sell to), and buyers are more likely to join/use the platform with each additional seller (more sellers to buy from), there can be diminished internal resistance to adding lower quality sellers.

Platforms that recognize this strategy may incentivize seller listings to stimulate further growth and increase profits but do so without adequate scrutiny. As just one incentive, many platforms create "frictionless entry" by reducing the costs for sellers and buyers to join, thereby increasing the likelihood that the platform will reach an efficient and highly profitable scale.

Platforms also generate value by opening previously unused (or less frequently used) markets. In addition, online platforms reduce transaction costs by streamlining the actual transaction; for example, buyers and sellers use a standardized transaction method that simplifies interactions with buyers and reduces the risk that the buyer will not pay.

For example, before the rise of e-commerce, secondhand products could be sold at garage sales or in classified newspaper advertisements. E-commerce created a process for allowing buyers and sellers to trade goods digitally, reducing transaction costs and creating a global marketplace for used, but too often counterfeit, products.

Another way platforms generate value is by aggregating information and reducing search costs. A buyer may search for a product, either by keyword or product category, at lower search cost than visiting brick-and-mortar stores. Because of this, sellers on digital platforms have consumer visibility well beyond the seller's natural geographical sales area.

In addition, consumers who have made a purchase may use tools provided by the marketplace to rate the product and the seller involved. These ratings create an important mechanism to facilitate future consumer trust in an otherwise unknown seller.

In principle, such a rating system provides a key to overcoming a common economic problem that might otherwise preclude sales: without a low-cost trust building feature that also communicates quality, and in a market with significant numbers of low-quality products, buyers may refuse to purchase any product at all, or would demand a lower price to reflect the uncertainty. One frequent result is that low cost counterfeits drive out high quality, trusted brands from the online marketplace. In practice, even the ratings systems across platforms have been gamed, and the proliferation of fake reviews and counterfeit goods on third-party marketplaces now threatens the trust mechanism itself.

Lower Startup and Production Costs

The relative ease of setting up and maintaining e-commerce websites makes online marketplaces a prime locale for the retailing of counterfeit and pirated goods. E-commerce retailers enjoy low fixed costs of setting up and maintaining web businesses and lower costs for carrying out normal business operations such as managing merchant accounts. These ventures can be set up quickly without much sophistication or specialized skills.

Some online platforms allow retailers to use pre-made templates to create their stores while other platforms only require that a seller create an account. These businesses face much lower overhead costs than traditional brick-and-mortar sellers because there is no need to rent retail space or to hire in-person customer-facing staff. Not only can counterfeiters set up their virtual storefronts quickly and easily, but they can also set up new virtual storefronts when their existing storefronts are shut down by either law enforcement or through voluntary initiatives set up by other stakeholders such as market platforms, advertisers, or payment processors.

In the production stage, counterfeiters keep costs low by stealing product secrets or technological knowledge, exploiting new production technologies, and distributing operations across jurisdictions. One method involves employees who sell trade secrets to a third party who, in turn, develops and sells counterfeit products based on the stolen secrets. Another method relies on an intermediary to steal a firm's product or technology. The use of intermediaries reduces the traceability to the counterfeiter.

Counterfeiting and piracy operations also take advantage of new low-cost production technologies. For example, the technological advances in modeling, printing and scanning technologies such as 3D printing reduce the barriers for reverse engineering and the costs of manufacturing counterfeit products.

Lower production costs can also be achieved through distributed production operations. One method involves manufacturing the counterfeit good in a foreign market to lower the chances of detection and to minimize legal liability if prosecuted. This can be combined with importation of

the counterfeit labels separately from the items, with the labels being applied to the products after both items arrive in the U.S.

In addition, it is much cheaper to manufacture illicit goods because counterfeit and pirated goods are often produced in unsafe workplaces with substandard and unsafe materials by workers who are often paid little—and sometimes nothing in the case of forced labor. Moreover, in the case of goods governed by Federal health and safety regulations, it often costs much less to produce counterfeit versions that do not meet these health and safety standards.

Lower Marketing Costs

Businesses that use only an internet presence as their consumer-facing aspect typically enjoy lower costs of designing, editing, and distributing marketing materials. Counterfeiters also benefit from greater anonymity on digital platforms and web sites and greater ease to retarget or remarket to customers. For example, counterfeiters use legitimate images and descriptions on online platforms to confuse customers, and they open multiple seller accounts on the platform so that if one account is identified and removed, the counterfeiter can simply use another.

The popularity of social media also helps reduce the costs of advertising counterfeit products. The nature of social media platforms has aided in the proliferation of counterfeits across all e-commerce sites. Instagram users, for example, can take advantage of connectivity algorithms by using the names of luxury brands in hashtags. Followers can search by hashtag and unwittingly find counterfeit products, which are comingled and difficult to differentiate from legitimate products and sellers.

Lower Distribution Costs

Traditionally, many counterfeit goods were distributed through swap meets and individual sellers located on street corners. With the rise of online platforms for shopping, customers can have products delivered to them directly.

Foreign entities that traffic in counterfeits understand how to leverage newer distribution methods better suited to e-commerce than the traditional trade paradigm (i.e., imports arriving via large cargo containers with domestic distribution networks). Today, mail parcel shipments, including through express consignments, account for more than 500 million packages each year.[16] Seizures in the small package environment made up 93 percent of all seizures in 2018, a 6 percent increase over 2017. From 2012 to 2016, the number of seizures from express consignment carriers increased by 105 percent, and the MSRP of those seizures had a 337 percent increase.[17] In contrast, seizures from cargo decreased by 36 percent from FY17 to FY18.

[16] https://www.cbp.gov/sites/default/files/assets/documents/2019-Apr/FY%202017%20Seizure%20Stats%20Booklet%20-%20508%20Compliant.pdf p. 14

[17] https://www.gao.gov/assets/690/689713.pdf?mod=article_inline p. 14

The International Chamber of Commerce found that counterfeiters use international air packages because the high volume of these packages makes enforcement more difficult.[18] A recent report by the OECD points out that distributing counterfeits across a series of small packages spreads the risk of detection, and lowers the loss from having one or more shipments seized, suggesting that losses to the counterfeiter on an ongoing basis would be within a tolerable range.[19]

The OECD report also notes that it is harder for authorities to detect counterfeits in small parcels than in shipping containers because cargo containers making entry at a maritime port provide customs officials with more information, well in advance of arrival. Moreover, the effort required for CBP to seize a shipment does not vary by size of the shipment, meaning that a package of a few infringing goods requires the same resources to seize as a cargo container with hundreds of infringing goods.

Section 321 of the Tariff Act of 1930 has likewise encouraged counterfeiters to favor smaller parcel delivery. Under Section 321, a foreign good valued at or less than $800 and imported by one person on one day is not subject to the same formal customs entry procedures and rigorous data requirements as higher-value packages entering the United States. This reduced level of scrutiny is an open invitation to exploit Section 321 rules to transport and distribute counterfeits.

Rules set by the Universal Postal Union (UPU) have historically contributed to the distortion in rates for delivery of international e-commerce purchases to the United States.[20] UPU reimbursement rates have underpriced domestic postage rates for small parcels. This market distortion made it cheaper for small package exports to the United States. from certain countries than would otherwise be economically feasible and has encouraged the use of the international postal mode over other shipment channels. The United States recently scored a historic victory when the UPU overhauled its terminal dues system[21], effectively eliminating this outdated policy.[22]

Consumer Attitudes and Perceptions

The sale of counterfeits away from so-called "underground" or secondary markets (e.g. street corners, flea markets) to e-commerce platforms is reshaping consumer attitudes and perceptions. Where in the past, consumers could identify products by relying on "red flag" indicators—such as a suspicious location of the seller, poor quality packaging, or discount pricing—consumers are now regularly exposed to counterfeit products in settings and under conditions where the articles appear genuine.

While the risks of receiving a counterfeit may have been obvious to a consumer purchasing items on street corners, with the rise of online platforms, it is not so obvious anymore. For example, it is

[18] https://cdn.iccwbo.org/content/uploads/sites/3/2015/03/ICC-BASCAP-Roles-and-Responsibilities-of-Intermediaries.pdf p. 32
[19] OECD/EUIPO (2018), *Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends, Illicit Trade*, OECD Publishing, Paris. https://doi.org/10.1787/9789264307858-en p. 77
[20] The UPU is a specialized agency of the United Nations that coordinates postal policies between 190 countries. Importantly, these treaties determine the cost of shipping between the various countries and offers low rates to mail originating from abroad, as compared to domestic postage rates.
[21] Universal Postal Union (2019), *Decisions of the 2019 Geneva Extraordinary Congress*, http://www.upu.int/uploads/tx_sbdownloader/actsActsOfTheExtraordinaryCongressGenevaEn.pdf
[22] https://www.nytimes.com/2019/09/25/business/universal-postal-union-withdraw.html

unlikely that anyone would set out to purchase a counterfeit bicycle helmet given the potential safety risks; however, such items are readily available to unsuspecting consumers on e-commerce websites.

Reports indicate that some third-party marketplace listings falsely claim to have certifications with health and safety standards or offer items banned by federal regulators or even the platforms themselves. Coupled with the inability of buyers to accurately determine the manufacturer or the origin of the product, it is challenging for buyers to make informed decisions in the e-commerce environment.

In 2017, MarkMonitor found that 39 percent of all unwitting purchases of counterfeit goods were bought through online third-party marketplaces.[23] Sellers on large well-known platforms rely on the trust that those platforms hosting of the marketplace elicits. The results of this survey indicate that bad actors selling counterfeit goods on legitimate online platforms erodes trust in both the brands and the platforms themselves.

In 2018, Incopro conducted a survey focusing on United Kingdom (UK) consumers who had unwittingly purchased counterfeit goods and how their perceptions of online marketplaces were affected as a result.[24] The results of this survey show that 26 percent of respondents reported that they had unwittingly purchased counterfeits. Of these, 41 percent reported that they had never received a refund after reporting a seller to online marketplaces.

In addition, roughly one-third of respondents reported that they would be less likely to buy a widely counterfeited product from an online marketplace while 46 percent reported no longer using a particular online marketplace after receiving counterfeit goods. Respondents also reported that, when trying to differentiate between genuine and counterfeit products, they consider online reviews along with the reputation of online marketplaces.

These recent findings, against the larger backdrop of the e-commerce environment, demonstrate the immediacy of the problem as consumer confidence and brand integrity continue to suffer in the realm of online third-party marketplaces.

Top Products Prone to Counterfeiting and Piracy

Counterfeiters sell fake goods as authentic goods — for example, a copy of a Louis Vuitton bag or Rolex watch fraudulently sold as the "real thing." Counterfeiters use identical copies of registered trademarks without the authorization of the rightful owner.

Piracy typically refers to the act of copying a protected work (such as a book, movie, or music) without the consent of the rights holder or person duly authorized by the rights holder.

[23]MarkMonitor (2017). *MarkMonitor Online Barometer: Global online shopping survey 2017 – consumer goods.* Downloaded from https://www.markmonitor.com/download/report/MarkMonitor_Online_Shopping_Report-2017-UK.pdf. p. 6
[24]INCOPRO, 2018. Counterfeit Products are Endemic – and it is damaging brand value: INCOPRO Market Research Report available at https://www.incoproip.com/cms/wp-content/uploads/2018/11/2018_Incopro_Market-Research-report.pdf.

The below table provides a summary of the annual IPR seizure statistics collected by CBP in FY18; including items from all modes of transportation. Apparel and other types of accessories, along with footwear, top the list at 18 percent and 14 percent of seizures, respectively. Commonly counterfeited items in these categories include brand name shoes such as Nike and Adidas, as well as NFL jerseys.

Watches and jewelry follow at 13 percent of total seizures. During the Mega Flex operation on August 21, 2019, for example, CBP officers seized counterfeit Rolex watches valued at over $1.4 million. Handbags and wallets represented nearly 11 percent of all seizures, including counterfeits of luxury brands such as Louis Vuitton, Michael Kors, and Gucci. Consumer electronics represented 10 percent of seizures, including products such as iPhones, hover boards, earbuds, microchips, and others.

Pharmaceuticals and personal care items account for only 7 percent of total seizures. However, as discussed in the next section, many of the products in these categories pose significant dangers to the consumer. Fake prescription drugs can lack active ingredients, contain incorrect dosages, or include dangerous additives. Fake personal care items such as cosmetics have been found to contain everything from harmful bacteria to human waste. Between 2017 and 2018, CBP and ICE Homeland Security Investigations (HSI) seized over $31 million in fake perfumes from China.

CBP Intellectual Property Rights Annual Seizure Statistics Fiscal Year 2018		
Products	**Seizures**	**Percent of Total**
1. Wearing Apparel/Accessories	6,098	18%
2. Footwear	4,728	14%
3. Watches/Jewelry	4,291	13%
4. Handbags/Wallets	3,593	11%
5. Consumer Electronics	3,388	10%
6. Consumer Products	2,816	8%
7. Pharmaceuticals/Personal Care	2,293	7%
8. Optical Media	561	2%
9. Toys	487	1%
10. Computers/Accessories	450	1%

Source: U.S. Customs and Border Protection

4. Health and Safety, Economic, and National Security Risks

Counterfeit trafficking exposes American consumers to significant health and safety risks — in addition to significant economic impacts and, in some cases, threats to national security.

Health and Safety

The types of counterfeit goods available on e-commerce platforms go far beyond those products with potential hidden toxins — like sports jerseys, jewelry and purses—and include many products

that can pose more obvious serious risks to health and safety, like prescription drugs and air bags. It is not only the sellers of the counterfeit goods, but also the e-commerce platforms and other third-party intermediaries (e.g., shippers) that facilitate their sale, that are profiting from the marketing and distribution of these illicit products to the American public.

The profit margins are especially high for counterfeiters in the sale of counterfeit pharmaceuticals. In the past, counterfeit prescription drugs primarily involved so-called lifestyle drugs like sildenafil (Viagra). Today, this market has expanded to include all types of therapeutic medicines, including insulin, cancer medications, and cardiovascular drugs.

Counterfeiting has also spread into over-the-counter medicines like cough syrup and weight loss drugs. As more Americans purchase drugs online, many U.S. consumers appear to be largely unaware of the potential dangers of purchasing counterfeit drugs from internet pharmacies.

Unlike legitimate drug manufacturers that are subject to inspections by the U.S. Food and Drug Administration, labs that manufacture counterfeits have no such oversight. According to a 2019 Better Business Bureau study, "companies based in China, Hong Kong, Singapore, and India shipped 97 percent of the counterfeit medicines seized in the U.S."[25]

In March 2019, Europol, the European Union's law enforcement agency, seized 13 million doses of counterfeit medicine ranging from opioids to heart medication. Europol noted that this type of counterfeiting is on the rise due to the relatively low risk of criminal detection.[26]

Counterfeit medicines not only defraud consumers who are often afflicted with serious health issues; they can also be lethal. Fake prescription opioids are often laced with deadly fentanyl, much of which originates in China. In raising awareness of the dangers, the National Institutes of Health (NIH) has warned:

> *Preventing counterfeit medicines from entering the United States is especially difficult, in part because nearly 40 percent of drugs are made overseas and approximately 80 percent of the active medicinal components of drugs are imported. Because many of these medicines are expensive, buyers are attracted by lower prices. The rise of Internet pharmacies makes regulation of drug safety more difficult.* [27]

---

[25]Baker, C. Steven, "Fakes are Not Fashionable: A BBB Study of the Epidemic of Counterfeit Goods Sold Online," *Better Business Bureau*, May 2019. https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st_louis_mo_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf

[26]Baker, C. Steven, "Fakes are Not Fashionable: A BBB Study of the Epidemic of Counterfeit Goods Sold Online," *Better Business Bureau*, May 2019. Pg. 9. https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st_louis_mo_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf

[27]National Institutes of Health, Blackstone, Erwin A., Joseph P. Fuhr Jr., and Steve Pociask, "The Health and Economic Effects of Counterfeit Drugs," *American Health and Drug Benefits* 7(4): 216-224, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4105729/; See also, Mackey, Tim K., et al., "After counterfeit Avastin®-- what have we learned and what can be done," *Nature Reviews Clinical Oncology* 12, 302-308. 2015. https://www.nature.com/articles/nrclinonc.2015.35.pdf

Health and safety risks extend far beyond fake prescription drugs. Counterfeit cosmetics often contain ingredients such as arsenic, mercury, aluminum, or lead and may be manufactured in unsanitary conditions, which can ultimately lead to problems with one's eyes or skin.

An investigation of counterfeit iPhone adapters conducted by the GAO found a 99 percent failure rate in 400 counterfeit adapters tested for safety, fire, and shock hazards, and found that 12 of the adapters posed a risk of lethal electrocution to the user.[28] In December 2015, CBP seized 1,378 hover boards with counterfeit batteries, which can cause fires resulting in injury or death.[29]

Children's toys, some laced with deadly metals like cadmium and lead, represent another area in which counterfeiters have taken advantage of e-commerce business models that provide limited to no accountability for sellers.

The Department of Justice has prosecuted individuals for the online sale of a "high value target" of counterfeiters — namely, airbags.[30] Along with other counterfeit automotive parts like brake pads, wheels, and seat belts, unsafe airbags can have catastrophic consequences for drivers, as well as for their passengers and others on the road. Bicycle helmets, another favorite of counterfeiters, likewise can lead to catastrophic consequences for cyclists.

Of the contraband products seized in 2016 by CBP and ICE/HSI, an astonishing 16 percent posed direct and obvious threats to health and safety.[31] E-commerce also facilitates the widespread sale of pirated versions of copyrighted works. Pirated medical books — which can contain errors that endanger patients' lives — have been found on platforms along with other pirated books (textbooks and trade books) and illicit reproductions of music-CD box sets.

Economic Harm

The growth in online sales of counterfeit and pirated goods directly harms — and unfairly competes against — the many legitimate companies that produce, sell and distribute genuine goods, often resulting in lost profits, employee layoffs, and diminished incentives to innovate. Frontier Economics (2018) finds that counterfeit goods displaced roughly half a trillion dollars of global sales of legitimate companies in 2013 and forecasts this displacement to reach $1 to $1.2 trillion by 2022.[32] The study also estimates that global employment losses due to counterfeit goods

[28]Underwriters Laboratory (UL), "Counterfeit iPhone Adapters", available at: https://legacy-uploads.ul.com/wp-content/uploads/sites/40/2016/09/10314-CounterfeitiPhone-WP-HighRes_FINAL.pdf. Also *see*, U.S. Government Accountability Office Report to the Chairman, Committee on Finance, U.S. Senate: *Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market*, GAO-18-216, Washington, DC: Government Accountability Office, January 2018. Pg.18. https://www.gao.gov/assets/690/689713.pdf

[29]U.S. Government Accountability Office Report to the Chairman, Committee on Finance, U.S. Senate: *Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market*, GAO-18-216, Washington, DC: Government Accountability Office, January 2018. https://www.gao.gov/assets/690/689713.pdf

[30]Department of Justice, U.S. Attorney's Office, Western District of New York, "Two Men Charged with Importing and Selling Counterfeit Airbags," 24 October 2016. https://www.justice.gov/usao-wdny/pr/two-men-charged-importing-and-selling-counterfeit-airbags; Department of Justice, U.S. Attorney's Office, Western District of New York, "Cheektowaga Man Sentenced for Buying and Selling Counterfeit Airbags," 9 May 2019.

[31]Department of Homeland Security, U.S. Customs and Border Protection, "Intellectual Property Rights: Fiscal Year 2018 Seizure Statistics," August 2019. https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR_Annual-Report-FY-2018.pdf

[32]https://iccwbo.org/publication/economic-impacts-counterfeiting-piracy-report-prepared-bascap-inta/

were between 2 million and 2.6 million jobs in 2013, with job displacement expected to double by 2022.

Counterfeit goods also damage the value of legitimate brands. When brand owners lose the ability to collect a price premium for branded goods, it leads to diminished innovation as brand owners are less likely to invest in creating innovative products. Legitimate companies, and particularly small businesses, report devastating impacts due to the abundance of competing online counterfeits and pirated goods. Moreover, while e-commerce platforms can benefit legitimate businesses by helping them to reach customers with a new product, the same process and technology also makes it easier for unscrupulous firms to identify popular new products, produce infringing versions of them, and sell these illicit goods to the business's potential customers.

As previously noted, the speed at which counterfeiters can steal intellectual property through e-commerce can be very rapid. If a new product is a success, counterfeiters may attempt to immediately outcompete the original seller with lower-cost counterfeit versions — while avoiding research and development costs. The result: counterfeiters may have a significant competitive advantage in a very short period of time over those who sell trusted brands.

Such fast-track counterfeiting poses unique and serious problems for small businesses, which do not have the same financial resources as major brands to protect their intellectual property. Lacking the ability to invest in brand-protection activities, such as continually monitoring e-commerce platforms to identify illicit goods, perform test buys, and send takedown notices to the platforms, smaller businesses are more likely to experience revenue losses as customers purchase counterfeit versions of the branded products.

In many cases, American enterprises have little recourse aside from initiating legal action against a particular vendor. Such legal action can be extremely difficult. Many e-commerce sellers of infringing products are located outside the jurisdiction of the United States, often in China; existing laws and regulations largely shield foreign counterfeiters from any accountability.

Organized Crime and Terrorism

The impact of counterfeit and pirated goods is broader than just unfair competition. Law enforcement officials have uncovered intricate links between the sale of counterfeit goods and transnational organized crime. A study by the Better Business Bureau notes that the financial operations supporting counterfeit goods typically require central coordination, making these activities attractive for organized crime, with groups such as the Mafia and the Japanese Yakuza heavily involved.[33] Criminal organizations use coerced and child labor to manufacture and sell counterfeit goods. In some cases, the proceeds from counterfeit sales may be supporting terrorism and dictatorships throughout the world.[34]

[33] https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st_louis_mo_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf

[34] United Nations Office of Drugs and Crime (UNODC), *Focus On: The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime*, available at: https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf

National Security

One of the greatest threats counterfeits pose to national security is their entry into the supply chain of America's defense industrial base. This defense industrial base includes both private sector contractors and government agencies, particularly the Department of Defense.

In FY 2018, 12 percent of DHS seizures included counterfeit versions of critical technological components, automotive and aerospace parts, batteries, and machinery. Each of these industrial sectors have been identified as critical to the defense industrial base, and thus critical to national security. One example drawn from a 2018 study by the Bureau of Industry and Security within the Department of Commerce featured the import of counterfeit semiconductors or "Trojan chips" for use in defense manufacturing and operations[35]. Such Trojan chips can carry viruses or malware that infiltrate and weaken American national security. The problem of counterfeit chips has become so pervasive that the Department of Defense has referred to it as an "invasion." Companies from China are the primary producers of counterfeit electronics.[36]

5. How E-Commerce Facilitates Counterfeit Trafficking

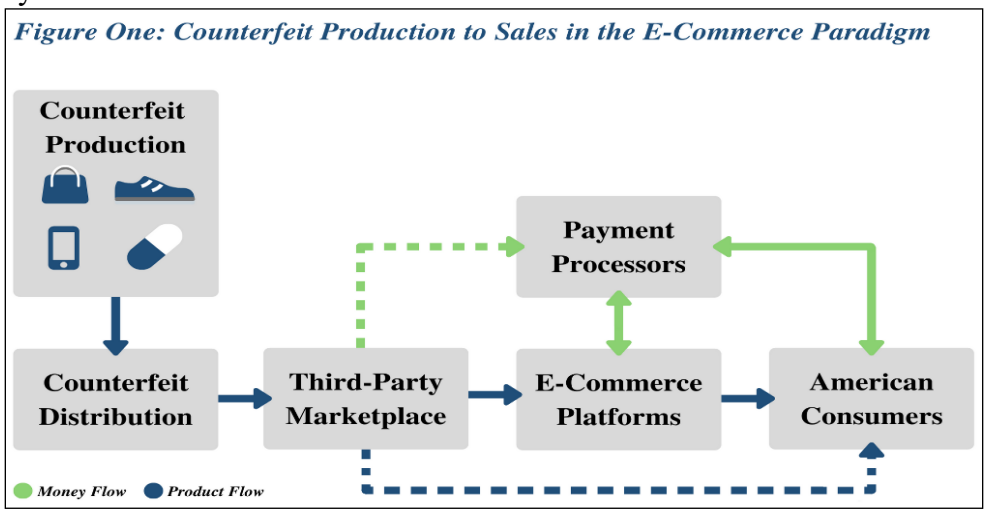
While e-commerce has supported the launch of thousands of legitimate businesses, e-commerce platforms, third-party marketplaces, and their supporting intermediaries have also served as powerful stimulants for the trafficking of counterfeit and pirated goods. The central economic driver of such trafficking is this basic reality: Selling counterfeit and pirated goods through e-commerce platforms and related online third-party marketplaces is a highly profitable venture.

For counterfeiters, production costs are low, millions of potential customers are available online, transactions are convenient, and listing goods on well-known platforms provides an air of legitimacy. When sellers of illicit goods are in another country, they are also exposed to relatively little risk of criminal prosecution or civil liability under current law enforcement and regulatory practices. It is critical that immediate action be taken to protect American consumers and other stakeholders against the harm and losses inflicted by counterfeiters.

[35] https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

[36] Saunders, Gregory and Tim Koczanksi, "Counterfeits," *Defense Standardization Program Journal*, October/December 2013. https://www.dsp.dla.mil/Portals/26/Documents/Publications/Journal/131001-DSPJ.pdf

Figure One provides a simplified overview of how counterfeit products move from production by counterfeiters to sales to American consumers:



Counterfeit Production and Distribution

The counterfeit sales process begins with some type of production capability for the counterfeit good. In this stage, counterfeiters enjoy enormous production cost advantages relative to legitimate businesses. Counterfeits are often produced in unsafe workplaces, with substandard and unsafe materials, by workers who are often paid little or sometimes nothing in the case of forced labor.

In the case of goods subject to federal health and safety regulations, it costs much less to produce counterfeit versions that do not meet these health and safety requirements that make the legitimate products so safe.

Counterfeiters likewise minimize the need for incurring significant research and development expenditures by stealing intellectual property, technologies, and trade secrets. They also shave production costs using inferior ingredients or components.

For example, a common way for counterfeiters to produce *fake* prescription opioids like Oxycontin, or a prescription drug like Viagra, is to start with the *real* pills as a basic ingredient. These real pills are then ground up into a powder, diluted with some type of (sometimes toxic) powder filler, and then "spiked" with an illegal and deadly narcotic like fentanyl, in the case of fake opioids, or illegal and deadly amphetamines or strychnine, in the case of Viagra.

In the case of apparel, such as running shoes, employees from a legitimate branded company may leave the company and set up their own facility. These employees have the expertise to manufacture identical-looking shoes; but they will typically do so with cheaper, inferior components. The result: the shoes may fail during activity, injure the user with an inferior insole, or, at a minimum, wear out faster than the real product.[37]

[37]Department of Homeland Security, U.S. Customs and Border Protection, "CBP Seizes Over $2.2 Million worth of Fake Nike Shoes at LA/Long Beach Seaport," 9 October 2019. https://www.cbp.gov/newsroom/local-media-release/cbp-seizes-over-22-million-worth-fake-nike-shoes-lalong-beach-seaport

The technological advances in modeling, printing, and scanning technologies such as 3D printing, have also significantly reduced the barriers for reverse engineering and the costs of manufacturing counterfeit products. Again, one problem that may arise may be the use of inferior production inputs that lead to product failure.

These are just a few of the many ways counterfeits begin their long journey into American households. There is often no way for legitimate businesses to compete, on a production cost basis, with counterfeiters. There is also often no way for a consumer to tell the difference between a counterfeit and legitimate good.

Third-Party Marketplaces and Counterfeiter Websites

A counterfeiter seeking to distribute fake products will typically set up one or more accounts on third-party marketplaces, and these accounts can often be set up quickly and without much sophistication or many specialized skills. Under such circumstances, it is axiomatic that online retailers face much lower overhead costs than traditional brick-and-mortar sellers. There is no need to rent retail space or to hire in-person, customer-facing staff.

In a common scenario, third-party marketplace websites contain photos of the real product, fake reviews of the counterfeit product, and other such disinformation designed to mislead or fool the consumer into believing the legitimacy of the product. The proliferation of such disinformation is the hallmark of the successful online counterfeiter. Such deception not only provides counterfeiters with an enormous competitive advantage over their brick-and-mortar counterparts; legitimate sellers on the internet are harmed as well.

In some cases, counterfeiters hedge against the risk of being caught and their websites taken down from an e-commerce platform by preemptively establishing multiple virtual store-fronts. A key underlying problem here is that on at least some e-commerce platforms, little identifying information is necessary for a counterfeiter to begin selling. In the absence of full transparency, counterfeiters can quickly and easily move to a new virtual store if their original third-party marketplace is taken down.

The popularity of social media also helps proliferate counterfeits across various e-commerce platforms. Instagram users, for example, can take advantage of connectivity algorithms by using the names of luxury brands in hashtags. Followers can search by hashtag and unwittingly find counterfeit products, which are comingled and difficult to differentiate from legitimate products and sellers.

According to a 2019 report, *Instagram and Counterfeiting*, nearly 20 percent of the posts analyzed about fashion products on Instagram featured counterfeit or illicit products.[38] More than 50,000 Instagram accounts were identified as promoting and selling counterfeits, a 171 percent increase from a prior 2016 analysis. Instagram's Story feature, where content disappears in twenty-four hours, was singled out as particularly effective for counterfeit sellers.

[38]Stroppa, Andrea*, et al*., "Instagram and counterfeiting in 2019: new features, old problems," *Ghost Data*, 9 April 2019. Rome, New York. https://ghostdata.io/report/Instagram_Counterfeiting_GD.pdf

A more recent development on social media is the proliferation of "hidden listings" for the sale of counterfeits. Social media is used to provide direct hyperlinks in private groups or chats to listings for counterfeit goods that purport to be selling unrelated legitimate items. By accessing the link, buyers are brought to an e-commerce platform which advertises an unrelated legitimate item for the same price as the counterfeit item identified in the private group or chat. The buyer is directed to purchase the unrelated item in the listing but will receive the sought-after counterfeit item instead.

Order Fulfillment in E-Commerce

The foreign counterfeiter must first choose between sending a package either by express consignment carrier or through the international post. As a general proposition, express consignment shippers — such as DHL Express, Federal Express, and the United Parcel Service — were subject to data requirements before they were extended to the international posts.

In the next step along the delivery chain, a parcel will arrive at a port of entry under the authority of CBP. Millions of parcels arrive daily, and it is impossible to inspect more than a very small fraction.

Although ocean shipping is still a major mode of transport for counterfeits, the rapid growth of other modes, such as truck and air parcel delivery, threaten to upend established enforcement efforts, and as such, is increasingly used by international counterfeiters. This continued shift from bulk cargo delivery to other modes by counterfeiters is illustrated in the trends in seizure statistics.

It is clear from these observations that counterfeit traffickers have learned how to leverage newer air parcel distribution methods that vary from the traditional brick-and-mortar retail model (for example, imports arriving via large cargo containers with domestic distribution networks). This is an issue that must be directly addressed by firm actions from CBP.

Section 321 De Minimis Exemption and Counterfeit Trafficking

Under Section 321 of the Tariff Act of 1930, as amended by the Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA), articles with a value of $800 or less, imported by one person on one day, can be admitted free of duty and taxes. Under 19 CFR § 10.151 and 19 CFR part 143, Subpart C, those importations are often not subject to the same formal customs procedures and rigorous data requirements as higher-value packages entering the United States. Instead, the low-value shipments can be admitted into U.S. commerce with the presentation of a bill of lading or a manifest listing each bill of lading and a limited data set. The relatively limited nature of the data requirements complicates the identification of high-risk goods by CBP and other enforcement agencies. Under 19 CFR § 143.22, CBP has existing authority to require formal entry (and the complete data set for any shipment) for any merchandise, if deemed necessary for import admissibility enforcement purposes; revenue protection; or the efficient conduct of customs business.

Warehouses, Fulfillment Centers and Counterfeit Trafficking

Certain e-commerce platforms have adopted a business model that relies on North American warehouses to provide space for foreign-made goods, followed by one-at-a-time order fulfillment, at which point the goods are individually packed and shipped to U.S. consumers on much shorter delivery timelines. The platforms that use this model may also coordinate with customs brokers, as well as provide third-party logistics and freight forwarding services to assist with the initial delivery of goods to the warehouse.

Although this model is a significant innovation for legitimate commerce and provides benefits to consumers in the form of reduced costs and shipping time, it creates a mechanism that allows counterfeit traffickers to minimize transportation costs as well, while intermingling harmful goods among legitimate goods. From a risk perspective, this model allows goods to enter the United States in a decentralized manner, allowing a counterfeit trafficker to spread the risk of seizure across a number of low-value packages. In situations where the fulfillment center is outside the U.S. Customs area, this model provides the opportunity to use ocean container shipping as the primary mode of transit for the shipment, which keeps overall shipping costs relatively low as ocean cargo is much cheaper than air delivery. It is in part because of these incentives that these fulfillment centers have emerged as an important element of the supply chains for many counterfeit traffickers.

6. Private Sector Outreach and Public Comment

This report benefitted from extensive outreach to, and comments from, numerous private sector stakeholders in response to the FRN 2019-14715 issued on July 10, 2019. Respondents included: e-commerce platforms that operate third-party marketplaces, third-party sellers, shippers, third-party logistics providers, payment processors, and intellectual property rights holders.

Rights holders and Stakeholders Feedback

In providing comments on platforms' current preventative efforts, rights holders argued that some platforms do not do enough to ensure that sellers provide accurate information. They also stressed that the onboarding and vetting of sellers remains a concern of the highest priority.

Some commenters further argued that sellers will not be sufficiently deterred unless they can be identified and punished for promoting counterfeit and pirated goods via online platforms. Further, they contended that platforms should be more proactive in their approach to combating IPR theft and misuse. Commenters also advised that the lack of relevant policies and procedures to verify sellers' true names and addresses, and to conduct the necessary vetting and due diligence, contributes to a range of impediments to effective enforcement.

Rights holders widely view the present legislative landscape for online enforcement — where online intermediaries are generally not strictly liable for the products sold on their marketplaces by third parties — to be out of date. While in the brick-and-mortar economy, contributory infringement liability has been well-developed through case law for the licensing and oversight of

sellers, a comparable regime is largely non-existent in the e-commerce realm. A key problem here is that the laws that apply today have remained largely unchanged since the early days of e-commerce. They were developed at a time when Congress' primary concern was to avoid over-regulation of the nascent market — as exemplified by the numerous safe harbors and limitations on liability for third-party intermediaries.

Rights holders further argued that the current rules, regulations, and practices governing e-commerce disproportionately place the burden of enforcement on rights holders. While e-commerce platforms that operate third-party marketplaces provide various tools for rights holders to report counterfeit listings of their brands, they have effectively shifted the primary responsibility to monitor, detect, and remove infringing products to the rights holders.

Commenters also noted several disparities across e-commerce platforms. For example, among third-party marketplaces that control who may list products on their site for sale, some scrutinize their sellers much more than others. Some allow anyone to sell a product if they provide basic information about themselves, such as credit card and tax identity information. Others require more detailed information, such as an existing online presence, proof that the seller is a business entity and not an individual, and that the seller has established customer support.

Submissions were also received from several platforms noting that they have invested heavily in proactive efforts to prevent counterfeits from reaching their online stores, and several commenters noted that some platforms have significant interactions with law enforcement to combat counterfeits trafficking. Additionally, there was concern expressed by some respondents that while several of the leading online platforms have built out substantial programs, mandating that these practices be adopted by all online platforms could have significant consequences for smaller competitors.

Observations in Support of Strong Government Action

Five observations emerged from this stakeholder outreach and a broader review of the e-commerce landscape: first, actions by the private sector components of the e-commerce supply, distribution, and sales chain will be critical to reducing the heavy volume of counterfeit and pirated goods circulating in the U.S. economy. This is particularly true for third-party marketplaces, which provide tools that producers of counterfeit and pirated goods can exploit.

With respect to such actions, platforms are increasingly developing methods to remove counterfeit listings and compensate consumers who have unwittingly purchased counterfeit goods. Platforms are also improving their capabilities to more quickly identify counterfeits as well as identify product sectors that are more vulnerable to counterfeiting.

Second, despite such actions, private stakeholders have fallen far short of adequately addressing the substantial challenges that must be surmounted if the trafficking of counterfeit and pirated goods is to be deterred. Such trafficking continues to grow both in the volume and array of goods trafficked. A key failing within the private sector is a lack of a commonly accepted set of best practices to combat counterfeit trafficking.

Third, rights holders are often burdened by e-commerce platforms that operate third-party marketplaces with a disproportionate share of the costs of monitoring, detection, and enforcement falling on rights holders. This burden falls heavily on smaller American enterprises that cannot spread the costs due to trademark infringements and brand enforcement over large sales and inventories.

Fourth, no amount of officers or government resources alone can stem this trafficking.

Fifth, absent the adoption of a set of best practices and a fundamental realignment of incentives brought about by strong government actions, the private sector will continue to fall far short in policing itself. Indeed, the current incentive structure tends to reward the trafficking in counterfeit and pirated goods more than these incentives help to deter such trafficking.

The next two sections of this report identify a set of strong government actions that DHS, in consultation with the interagency, believes is necessary to bring about this fundamental realignment of incentives — and thereby ensure that e-commerce stakeholders appropriately shoulder much more of the responsibility for preventing the online trafficking in counterfeit and pirated goods.

7. Immediate Action by DHS and Recommendations for the USG

CBP and ICE are the primary federal agencies responsible for securing America's borders. A key responsibility is to prevent goods that infringe U.S. copyrights, registered trademarks, and certain patents from entering the United States. CBP's interdiction of counterfeit goods at U.S. Ports of Entry (POE) is the frontline of USG IPR enforcement.

In meeting their responsibilities, CBP and ICE have the statutory authority to inspect *any* package as it is imported into U.S. territory. CBP and ICE may draw upon numerous other authorities to stop and prevent the trafficking of counterfeit and pirated goods, from the assessment of civil fines and other penalties to debarring and suspending irresponsible actors. Many of these authorities are underutilized or underdeveloped to match the risks in the evolving e-commerce environment.

The previous sections of this report have provided an overview of the counterfeit trafficking landscape and identified key problems that need to be addressed firmly and swiftly. This section identifies a set of actions DHS will make through enforcement actions, sub-regulatory changes, and as necessary, notice and comment rulemaking or requested statutory amendments. These actions are summarized in the following table:

Immediate Actions to be Taken by DHS and Recommendations for the U.S. Government
1. Ensure Entities with Financial Interests in Imports Bear Responsibility
2. Increase Scrutiny of Section 321 Environment
3. Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Posts
4. Apply Civil Fines, Penalties and Injunctive Actions for Violative Imported Products

Unless the trafficking of counterfeit and pirated goods is greatly reduced, Americans will continue to face unacceptably high health and safety risks, American enterprises and workers will continue to endure severe negative impacts, innovation and economic growth will suffer, and America will continue to be exposed to significant national security risks.

1. Ensure Entities with Financial Interests in Imports Bear Responsibility

DHS will pursue a modernized enforcement and regulatory framework that reflects the economic realities of international e-commerce and ensures that the flow of contraband is stopped at its source.

- CBP will adjust its entry processes and requirements, as necessary, to ensure that all appropriate parties to import transactions are held responsible for exercising a duty of reasonable care.

- CBP will treat domestic warehouses and fulfillment centers as the ultimate consignee for any good that has not been sold to a specific consumer at the time of its importation. As discussed in this report, counterfeit products evade detection and sit in fulfillment centers waiting for purchase by a consumer. By treating domestic warehouses and fulfillment centers as consignees in such circumstances, CBP can enhance their ability to identify Section 321 abuses consistent with current authorities, as well as use its other statutory and regulatory authorities to combat trafficking of counterfeit goods in the possession of domestic warehouses and fulfillment centers.

- DHS will encourage platforms and other third-party intermediaries that own or operate warehouses or fulfillment centers to pursue, in coordination with rights holders, bulk abandonment and destruction of contraband goods that were not interdicted by CBP but are in the platform's or other third-party intermediary's possession in a warehouse or fulfillment center. In cases where CBP suspects merchandise destined for a U.S. fulfillment center violates trade laws prohibiting importation of counterfeit goods and initiates a seizure process for merchandise, CBP will notify the platform or other third-party intermediary operating the fulfillment center or warehouse and request they pursue abandonment and destruction with the rights holders of any identical offending goods in their possession. Failure to cooperate following such notification could be a factor when CBP and ICE identify counterfeit cases to pursue under their existing authorities.

- CBP will require formal entry for shipments deemed high-risk, notwithstanding that such shipments might otherwise qualify for duty-free or informal entry treatment. High-risk merchandise shall include those categories of goods that pose an elevated risk of counterfeiting and shall consider the source of the merchandise.

- CBP will address such high-risk shipments within its current bonding regime, developing a framework for a new type of bond specifically for counterfeit risk (like bonds required for anti-dumping and countervailing duties).

- In consultation with the Department of Justice, CBP will provide guidance regarding the types of customs violations that could be actionable under the False Claims Act (FCA) and will make information regarding successful FCA claims publicly available to inform and enable the public to identify and bring such violations to the attention of the government.

2. Increase Scrutiny of Section 321 Environment

As described above, existing laws and administrative practices may not sufficiently define responsibilities in the e-commerce environment, including who within an e-commerce transaction bears responsibility and legal liability for illicit merchandise and other violations. Statutes and administrative practices can be clarified and updated to provide greater transparency and information about the various parties involved so that DHS can identify high-risk transactions, interdict dangerous merchandise, and cause bad actors to pay the price for their actions. To address this problem in the Section 321 environment, CBP shall require data that sufficiently identifies the third-party seller and the nature and value of the imported merchandise, as well as other information that is necessary to determine the responsible party for Section 321 eligibility purposes, consistent with existing legal authorities. This will be informed by the following efforts:

- **Gather Information through Pilot Program.** CBP has been examining different e-commerce platform business models and has initiated several pilot programs designed to better understand the dynamics involved, and the type of information that the government should be collecting, including the "Section 321 Data Pilot" specifically for Section 321 entries, 84 Fed Reg. 35405 (July 23, 2019). CBP plans to continue these efforts for approximately two years and will use the information gained to better target counterfeits in the Section 321 environment, to help shape the scope of further policy formation, and ensure compliance with customs laws.

- **Enhanced Data Requirements.** Upon collection of adequate amounts of data through the Section 321 Data Pilot to identify gaps in the current data collection framework, but no later than six months from the issuance of this report, CBP will, consistent with applicable law, take all necessary steps — including, as applicable, issuing a notice of proposed rulemaking — to initiate a new data collection process. This process will include collecting certain information from domestic warehouses or fulfillment centers about third-party sellers in transactions for which the third-party seller utilizes a domestic warehouse or fulfillment center to store inventory for further sale to domestic consumers. The collection will also include data that sufficiently identifies the third-party seller and the nature and

value of the imported merchandise, as well as other information that is necessary to determine the responsible party for Section 321 eligibility purposes, consistent with existing legal authorities. As appropriate, the domestic warehouse or fulfillment center may be deemed the "person" for Section 321 eligibility if the warehouse or fulfillment center fails to provide CBP with such information.

- **Issue Guidance.** To prevent abuse of Section 321, CBP will develop administrative guidance and, if necessary, consider whether promulgating new regulations is necessary to better define and subsequently enforce Section 321 eligibility requirements. At a minimum this guidance will address the following:

    - What value needs to be reported for a Section 321 entry; and

    - What information will be necessary to uniquely identify the ultimate consignee.

3. Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Postal Operators

In appropriate circumstances, CBP and ICE currently take steps to add persons (both entities and individuals) that have been found to lack present responsibility to the federal suspension and debarment list. Those persons on this suspension and debarment list are prohibited from participating in both government procurement and certain other non-procurement activities. However, current agency practices continue to permit these persons to obtain importer of record numbers and import goods into the United States.

Explicitly clarifying the scope of suspension and debarment to prevent participation in the importer of record program by amending Executive Order 12549 will assist CBP in requiring regulated entities to screen their customers against the suspension and debarment list. This will improve targeting and reduce the number of packages sent by repeat offenders, thereby stopping the flow of contraband at their sources.

- CBP recommends amending Executive Order 12549 to explicitly bar suspended and debarred persons from participating in the Importer of Record Program.

- Following such an amendment, or as otherwise consistent with applicable law and Executive Orders, CBP will require express consignment operators, carriers, and hub facilities to verify their customers have not been suspended or debarred from participating in the Importer of Record Program and refuse to provide import-related services to such suspended or debarred customers.

- Consistent with applicable law, CBP will condition continued access to its "trusted trader programs" by express consignment operators, carriers, and hub facilities on compliance with this verification process that determines whether a customer has been suspended or debarred.

- Consistent with applicable law, CBP also will identify non-compliant international postal operators and international posts by developing an International Mail Non-Compliance metric and will take enforcement actions based on these metrics.

4. Apply Civil Fines, Penalties, and Injunctive Actions for Violative Imported Products

It is critical to the integrity of e-commerce and for the protection of consumers and rights holders that e-commerce platforms that operate third-party marketplaces, and other third-party intermediaries assume greater responsibility, and therefore greater liability for their roles in the trafficking of counterfeit and pirated goods. To that end, CBP and ICE will use existing statutory and regulatory authorities to reach the activities of third-party marketplaces and other intermediaries where evidence demonstrates they have unlawfully assisted in the importation of counterfeit and pirated goods through the following actions:

- CBP and ICE will immediately begin to identify cases in which third-party intermediaries have demonstrably directed, assisted financially, or aided and abetted the importation of counterfeit merchandise. In coordination with the Department of Justice, CBP and ICE will seek all available statutory authorities to pursue civil fines and other penalties against these entities, including remedies under 19 U.S.C. § 1526(f), as appropriate.

- DHS recommends the administration pursue a statutory change to explicitly permit the government to seek injunctive relief against third-party marketplaces and other intermediaries dealing in counterfeit merchandise.

- In the interim, DHS will provide information and support to registered brand owners looking to utilize statutory authorities to seek injunctive relief against persons dealing in counterfeit merchandise, whether through direct sales or facilitation of sales, following seizures of goods that are imported contrary to law.

- ICE shall prioritize investigations into intellectual property-based crimes regardless of size and will make referrals for all such investigations where appropriate.

- ICE will coordinate with the Department of Justice to develop a strategy to investigate and prosecute intellectual property violations at all levels of the supply chain at a sufficiently high level to respond to the concerns raised in this report and according to its budget and broader mission goals.

5. Leverage Advance Electronic Data for Mail Mode

The United States Postal Service (USPS) is responsible for the presentation of mail and the provision of advance electronic data (AED) to CBP for arriving international mail parcels. USPS receives such AED from international posts. As has been noted, given the number of e-commerce transactions that are sent by mail, there is a significant gap in the information CBP receives. USPS and CBP have enhanced their collaboration in the targeting and identification of offending

merchandise that is imported through international mail. Both agencies are implementing new strategies for leveraging the AED already available to identify offending merchandise by taking the following actions:

- DHS and USPS have signed a letter of intent that enables the USPS to work alongside CBP during special operations to become a force multiplier in the interdiction of counterfeit products.

- Upon completion and publication of the Synthetics Trafficking and Overdose Prevention (STOP) Act implementing regulations, DHS will use information gleaned from the 321 Data Pilot and will make recommendations to USPS to address any critical data gaps that remain between what is required of mail versus air cargo. At a minimum, this effort will seek to enhance the individualized tracking of international mail parcels sent through air cargo.

6. Plan for ACTION

Counterfeit networks can be complex and multidimensional, exploiting legal and regulatory nuances in the different stages and aspects of international trade. Yet, for a variety of reasons, including competition law and trade secrets protection, various stakeholders in the e-commerce supply and distribution chains historically have not shared information on problematic sellers, shippers, freight forwarders, brokers, and other third-party intermediaries involved in counterfeit trafficking.

To address this issue, the IPR Center established the E-Commerce Working Group (ECWG) to foster and encourage the flow of actionable data and information between platforms and relevant third-party intermediaries as well as affected carriers, shippers, search engines, and payment processors. DHS supports the efforts of the IPR Center's ECWG and recommends the formation of the Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION). Specific ACTION efforts will include the following:

- Sharing information within the ACTION framework on sellers, shippers, and other third-party intermediaries involved in trafficking in counterfeit and pirated goods.

- Sharing of risk automation techniques allowing ACTION members to create and improve on proactive targeting systems that automatically monitor online platform sellers for counterfeits and pirated goods.

- In addition, ACTION members may enter non-binding memoranda of understanding (MOU) with the IPR Center, consistent with U.S. law, to clarify the expectations and legal understanding for data sharing and coordinated IPR enforcement moving forward. Such MOUs will provide a vehicle to create a compliance scoring mechanism, as well as to delineate reasonable efforts to know the seller as well as the scope of products involved

(e.g., fast-moving consumer goods, consumer electronics, fashion and luxury products, sports goods, software, and games, and toys).

7. Analyze Enforcement Resources

Packages shipped through the international mail environment account for approximately 500 million packages annually. This does not include the millions of packages sent out daily via express consignment carriers. Amidst this flood of packages, insufficient resources can create a key limitation on the capabilities of DHS and other government agencies to screen, target, and detect the counterfeit and pirated goods that hide amongst the increasing massive flow of small packages.

A lack of resources also limits the ability of intelligence gathering and analysis, the proper determination of whether suspect goods may be counterfeit, the collection of comprehensive data on the trafficking in counterfeit and pirated goods, and the ability to conduct criminal investigations into the organizations that traffic in counterfeit goods. To address these issues, the following actions shall be taken:

- CBP will analyze whether the fees collected by CBP are currently set at sufficient levels to reimburse the costs associated with processing, inspecting, and collecting duties, taxes, and fees for parcels. CBP shall also provide recommendations to the Department of the Treasury regarding any fee adjustments that would be necessary to fund and reimburse the federal government's costs for more effectively combating the trafficking of counterfeit and pirated goods.

8. Create Modernized E-Commerce Enforcement Framework

DHS will pursue a modernized enforcement framework that reflects the economic realities of international e-commerce. This new framework may rely on the provision of privileges or benefits by CBP to e-commerce entities in exchange for the submission of additional data elements and sufficient internal controls that demonstrate the entities' ability to identify and manage risk within their respective supply chains. This new framework may also require updates to existing statutes and regulations to underpin this effort. Key elements of a modernized e-commerce enforcement framework could include, but are not limited to:

- Seeking statutory authority to treat IPR infringing goods as summarily forfeited upon discovery by CBP or ICE similar to the treatment of Schedule I and II narcotics under Title 21 of the U.S. Code. This will send a clear message about the importance of IPR enforcement, and simultaneously streamline the disposition of CBP enforcement actions.

- Pursuing statutory and/or regulatory changes, as necessary, so that CBP can better share information with the private sector;

- Implementing a risk-based bonding regime for e-commerce transactions; and

- Adopting streamlined enforcement processes for seized, abandoned, and forfeited goods.

9. Assess Contributory Trademark Infringement Liability for E-Commerce

Online platforms have avoided civil liability for contributory trademark infringement in several cases. Given the advance and expansion of e-commerce, DHS recommends that the Department of Commerce consider the following measures:

- Assess the state of liability for trademark infringement considering recent judicial opinions, and the impact of this report—including platforms' implementation of the best practices directed herein.

- Seek input from the private sector and other stakeholders as to the application of the traditional doctrines of trademark infringement to the e-commerce setting, including whether to pursue changes in the application of the contributory and/or vicarious infringement standards to platforms.

10. Re-Examine the Legal Framework Surrounding Non-Resident Importers

Currently, non-resident importers can legally enter goods into the United States provided they have a "resident agent" as defined in regulation. In practice, it can be difficult to compel non-resident importers to pay civil penalties and respond to other enforcement actions available to the USG. With this in mind, DHS should reevaluate the legal framework for allowing non-resident importers in the Section 321 *de minimis* low-value shipment environment.

11. Establish a National Consumer Awareness Campaign

Given the critical role that consumers can play in the battle against online counterfeiting, DHS recommends the development of a national public-private awareness campaign. The national public awareness campaign recommended by DHS should involve platforms, rights holders, and the applicable government agencies to provide education for consumers regarding the risks of counterfeits as well as the various ways consumers can use to spot counterfeit products. At present, many consumers remain uninformed as to the risks of buying counterfeit and pirated products online. These risks are both direct to them (e.g., tainted baby food), as well as indirect (e.g., sales revenues can fund terrorism).

Many consumers are also unaware of the significant probabilities they face of being defrauded by counterfeiters when they shop on e-commerce platforms. As this report has documented, these probabilities are unacceptably high and appear to be rising. Even those consumers motivated to conduct research and stay informed might lack the specialized knowledge and efficient user tools to make diligent online buying decisions.

A strong and ongoing national campaign to increase public awareness about the risks of counterfeits in an e-commerce world should help alert consumers about the potential dangers of some online purchases. To the extent e-commerce platforms empower their consumers to participate in the monitoring and detection of counterfeits, e.g., by implementing several of the best practices recommended in this report, this will also help in the fight against the trafficking in counterfeit and pirated goods.

This effort could use technology as well as provide online education. For example, online marketplaces could prominently display messages on their home pages, as well as on high-risk item pages, warning customers about the dangers of counterfeits and urging respect for intellectual property rights. Additionally, the campaign could be paired with technologically-enabled assurances of authenticity. Such an approach would provide commercial advantages to the platforms that adopt it while also benefiting consumers and rights holders through reliable methods to identify and certify the authenticity of branded products across online platforms.

8. Private Sector Best Practices

The following table catalogs a set of high priority "best practices" that should be swiftly adopted by e-commerce platforms that operate third-party marketplaces, and other third-party intermediaries. Under the authority of the Secretary of the Department of Homeland Security, these best practices shall be recommended and communicated to all relevant private sector stakeholders by the ICE/HSI-led IPR Center.

It shall be a duty of the IPR Center to encourage, monitor, and report on the adoption of, and the progress and effectiveness of, these best practices, through all means necessary within the scope of the legal authority of DHS and the Federal Government.

Best Practices for E-Commerce Platforms and Third-Party Marketplaces
1. Comprehensive "Terms of Service" Agreements
2. Significantly Enhanced Vetting of Third-Party Sellers
3. Limitations on High Risk Products
4. Efficient Notice and Takedown Procedures
5. Enhanced Post-Discovery Actions
6. Indemnity Requirements for Foreign Sellers
7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests
8. Pre-Sale Identification of Third-Party Sellers
9. Establish Marketplace Seller IDs
10. Clearly Identifiable Country of Origin Disclosures

1. Comprehensive "Terms of Service" Agreements

It is critical that platforms require all third-party sellers to sign comprehensive and stringent terms of service agreements that maximize the authorities of the platforms to combat counterfeit

trafficking. Terms of service agreements will provide platforms with an important legal means to combat counterfeit trafficking

Most obviously, these terms of service should incorporate explicit prohibitions on selling counterfeit and pirated goods. Once the platform has affirmatively detected infringement on a seller profile, the actions listed below under the category of "post-discovery actions" should be allowed under the terms and taken swiftly.

The terms of service should also list the potential repercussions sellers face for violations. Generally, these repercussions should allow platforms to impose sanctions such as suspension, termination, and debarment without waiting for a determination by a court for sellers who violate the terms of the agreement. The terms should include escalating capabilities to suspend, terminate, and debar counterfeit traffickers and their affiliates.

Specifically, they should allow the platform to conduct, at a minimum, the following actions in response to violations or identified risk factors in the seller's profile and product postings without waiting for a determination by a court:

> (1) terminate or suspend a seller account based on the use or reference to a username that is confusingly similar to a registered trademark;
>
> (2) take down or suspend and keep down individual product postings based on the misuse of photographs, logos, external links to infringing content, certain coded messages with actual intellectual property references removed, or imbedded offers to manufacture; and
>
> (3) allow for an escalating enforcement structure that results in (for major infractions and/or repeat minor infractions) permanent removal of the seller, and any known related seller profiles, from the marketplace feature of the platform and further results in forfeiture and destruction of all offending goods in warehouses or fulfillment centers operated by, or under the control of, the platform.

To maximize platform authorities, and as explained further below, such terms of service should also allow platforms to impose appropriate limitations on products listed, require clearly identifiable country of origin disclosures, impose U.S. banking and indemnity requirements, and significantly improve pre-sale identification of third-party sellers.

2. Significantly Enhanced Vetting of Third-Party Sellers

Significantly enhanced vetting of third-party sellers is one of the most effective forms of due diligence platforms can engage in to reduce the risk of counterfeits entering the e-commerce stream. Platforms should have a uniform and articulable vetting regime to determine if a seller will be allowed to list products for sale.

To facilitate enhanced vetting, platforms should, at a minimum, require the following:

(1) sufficient identification of the seller, its accounts and listings, and its business locations prior to allowing the seller to list products on the platform;

(2) certification from the seller as to whether it, or related persons, have been banned or removed from any major e-commerce platforms, or otherwise implicated in selling counterfeit or pirated products online; and

(3) acknowledgment, where applicable, that the seller is offering trademarked products for which the seller does not own the rights (either because they are a reseller or seller of used products).

Information provided by potential sellers should also be vetted for accuracy, including through the following efforts:

(1) use of technological tools, as well as analyses of historical and public data, to assess risk of sellers and products; and

(2) establishment of an audit program for sellers, concentrating on repeat offenders and those sellers exhibiting higher risk characteristics.

Any failure to provide accurate and responsive information should result in a determination to decline the seller account and/or to hold the seller in violation of the platform's terms of service.

3. Limitations on High Risk Products

Platforms should have in place protocols and procedures to place limitations on the sale of products that have a higher risk of being counterfeited or pirated and/or pose a higher risk to the public health and safety. For example, some of the major platforms completely prohibit the sale of prescription medications by third-party sellers in their marketplaces. Many platforms also ban the sale of products that are known to be particularly vulnerable to counterfeiting and that pose a safety risk when sold online. Examples include car airbag components, infant formula, and new batteries for cellular phones.

Platforms can also place other types of restrictions on third-party sellers before certain high-risk categories of goods may be sold. For example, some platforms require prior approval for items such as automotive parts, jewelry, art, food, computers, sports collectibles, DVDs, and watches that are particularly prone to counterfeiting.

Platforms should prominently publish a list of items that may not be sold on third-party marketplaces under any circumstances (prohibited), as well as a list of items that can only be sold when accompanied by independent third-party certification (restricted). In constructing these lists, platforms should consider, among other things, whether a counterfeit version of the underlying product presents increased risks to the health and safety of U.S. residents or the national security of the United States. When a seller claims their merchandise has an independent third-party certification, and this certification is required in order for the product to be legally offered for sale

in the United States, platforms should make good-faith efforts to verify the authenticity of these certifications.

4. Efficient Notice and Takedown Procedures

Notice and takedown is the most common method of removing counterfeit listings from third-party marketplaces and e-commerce platforms. This noticing process can be particularly time-consuming and resource-intensive for rights holders who currently bear a highly disproportionate share of the burden of identifying the counterfeit listings for noticing.

These rights holders must invest significant resources to scour millions of listings across multiple platforms to identify potentially counterfeit listings and notify the third-party marketplace or e-commerce platform. This kind of comprehensive policing of e-commerce often is not possible for smaller enterprises.

As a further burden, some third-party marketplaces require rights holders to buy the suspected products from the sellers to verify that they are in fact counterfeit. There often is a delay of a day or longer between the time that notice is provided, and the time listing is removed. During this period, counterfeiters may continue to defraud American consumers.

To address these abuses — and assume a much greater share of responsibility for the policing of e-commerce — platforms should create and maintain clear, precise, and objective criteria that allow for quick and efficient notice and takedowns of infringing seller profiles and product listings. An effective regime should include, at a minimum, the following: (1) minimal registration requirements for an interested party to participate in the notice and takedown process; (2) reasonable rules that treat profile owners offering large quantities of goods on consumer-to-consumer platforms as businesses; and (3) transparency to the rights holders as to how complaints are resolved along with relevant information on other sales activity by the seller that has been implicated.

5. Enhanced Post-Discovery Actions

Upon discovery that counterfeit or pirated goods have been sold, platforms should conduct a series of "post-discovery" actions to remediate the fraud. These should include:

(1) notification to any buyer(s) likely to have purchased the goods in question with the offer of a full refund;

(2) notification to implicated rights holders, with details of the infringing goods, and information as to any remaining stock of the counterfeit and pirated goods held in warehouses;

(3) implementation of practices that result in the removal of counterfeit and pirated goods within the platform's effective control and in a manner that prevents such goods from re-entering the U.S. or being diverted to other markets; and

(4) immediate engagement with law enforcement to provide intelligence and to determine further courses of action.

6. Indemnification Requirements for Foreign Sellers

For a large portion of e-commerce, foreign sellers do not provide security or protection against a loss or other financial burden associated with the products they sell in the United States. Because these sellers are located outside the United States, they also may not be subject to the jurisdiction of U.S. courts in civil litigation or government enforcement actions. Further adding to this liability gap, there is this: while e-commerce platforms generally have a U.S. presence and are under U.S. jurisdiction, under the current interpretations of American laws and regulations, they are often found not to be liable for harm caused by the products they sell or distribute.

The result of this jurisdictional and liability gap is that consumers and rights holders do not have an efficient or predictable form of legal recourse when they are harmed by foreign products sold on third-party marketplaces. Accordingly, e-commerce platforms should require foreign sellers to provide some form of security in cases where a foreign product is sold to a U.S. consumer. Such form of security should be specifically designed to cover the potential types and scope of harm to consumers and rights holders from counterfeit or pirated products.

Note that there are several ways that platforms might flexibly achieve this goal. For example, requiring proof of insurance would provide a form of security for any reasonably foreseeable damages to consumers that might flow from the use of the product. Rights holders could also be compensated in cases of infringement.

7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests

Many foreign sellers on third-party marketplaces do not have a financial nexus to the United States, making it difficult to obtain financial information and to subject all parts of the transaction to U.S. law enforcement efforts.

Platforms should close this loophole by encouraging all sellers to clear transactions only with banks and payment providers that comply with U.S. law enforcement requests for information and laws related to (relevant to) the financing of counterfeit activity.

8. Pre-Sale Identification of Third-Party Sellers

Stakeholders have, at times, reported that buyers have been surprised to discover upon completion of an online sales transaction, that the order will be fulfilled by an unknown third-party seller and *not* the platform itself. Without addressing the separate legal question of whether this comprises deceptive action *per se*, at least some buyers may have made different purchasing decisions if they

had known, prior to purchase, the identity of the third-party "storefront" owner, and/or the party ultimately responsible for fulfilling the transaction.

To increase transparency on this issue, platforms should significantly improve their pre-sale identification of third-party sellers so that buyers can make informed decisions, potentially factoring in the likelihood of being sold a counterfeit or IPR infringing merchandise. Platforms should implement additional measures to inform consumers, prior to the completion of a transaction, of the identity of storefront owners and/or those responsible for fulfilling a transaction, as well as any allegations of counterfeits being sold by a particular seller. On the converse, if a particular seller is a licensed reseller of the product, this information should also be provided.

Even if this information may be currently available, firm steps should be taken to ensure that this information is featured prominently in product listings. This will prompt greater consumer awareness and lead to more informed decision-making.

9. Establish Marketplace Seller IDs

Platforms generally do not require a seller on a third-party marketplace to identify the underlying business entity, nor to link one seller profile to other profiles owned by that same business, or by related businesses and owners. In addition, the party that appears as the seller on the invoice and the business or profile that appears on the platform to be the seller, may not always be the same. This lack of transparency allows one business to have many different profiles that can appear unrelated. It also allows a business to create and dissolve profiles with greater ease, which can obfuscate the main mechanism that consumers use to judge seller credibility, namely reviews by other buyers.

Platforms should require sellers to provide the names of their underlying business or businesses (if applicable), as well as any other related seller profiles owned or controlled by that seller or that clear transactions through the same merchant account. Platforms can use this seller ID information in three helpful ways:

First, to communicate to the consumer a more holistic view of "who" is selling the goods, allowing the consumer to inspect, and consult reviews of, all related seller profiles to determine trustworthiness. Second, linking all related sellers together will assist rights holders in monitoring who is selling goods that they believe to be infringing. Third, the platform can use the connections to other seller profiles to better conduct its own internal risk assessment, and make risk mitigation decisions (e.g., requiring cash deposits or insurance) as appropriate based on the volume and sophistication of the seller.

10. Clearly Identifiable Country of Origin Disclosures

Brick-and-mortar retail stores are required to have labels on their products that clearly identify the country or countries of origin. No such requirement applies to online e-commerce.

Platforms should require sellers to disclose the country of origin of their products; and platforms should post this country of origin information for all the products they sell. This will assist both the platforms and consumers in evaluating the risks that a product might be counterfeit.

9. Conclusions

Both private sector and USG input to this report have shown that the flood of counterfeit and pirated goods now being trafficked to American consumers through online third-party marketplaces is threatening both the public health and safety as well as national security. The lack of effective methods for addressing counterfeit goods stifles American innovation and erodes the competitiveness of U.S. manufacturers and workers. Despite increased efforts of both the USG and private sector stakeholders, the trafficking of counterfeit and pirated goods continues to worsen, in both the volume and the array of products being trafficked.

This report to President Donald J. Trump has identified a set of strong government actions that DHS and other federal agencies can begin executing immediately to address a crisis that is undermining America's trust in e-commerce even as it is exposing the American public to undue and unacceptable risks.

Additionally, this report has proposed a set of best practices for private sector stakeholders that DHS believes should be adopted swiftly. As the longstanding experiences of brick-and-mortar stores demonstrate, the private sector is capable of operating businesses that sell legitimate, not illicit, goods to American consumers. We should expect the same level of care from online third-party marketplaces that we expect from the stores physically located in our communities.

During the time you have spent reading this report, hundreds of thousands of new clicks in online third-party marketplaces have started the process for a new wave of counterfeits flooding into the United States. Although the USG will continue to benefit from additional information flowing from current-running pilot programs, and longer-term legislative and regulatory efforts, the time has come for action, both from the USG and those private sector companies that desire to be good partners in combating the scourge of counterfeiting.

10. Appendix A: The IPR Center

The National Intellectual Property Rights Coordination Center (IPR Center) is led by Homeland Security Investigations. The IPR Center plays an important role in consumer and rights holders education on the dangers of purchasing counterfeit goods and on how to report a suspected counterfeit to law enforcement.

In 2018, the IPR Center conducted 192 IPR and commercial fraud-related outreach efforts, reaching 12,061 people. As recommended in this report, this IPR Center should play a critical and expanded role in the ongoing battle against counterfeit trafficking.

This Appendix describes some of the major initiatives the IPR Center is currently involved in.

Background on the IPR Center

The IPR Center brings together 25 U.S Government and foreign government agencies in a task force setting using a three-pronged approach to combat intellectual property and trade crime: interdiction, investigation, and outreach to the public and law enforcement. It seeks to coordinate a unified USG response to the growing threat of counterfeiting and has significantly expanded the original multi-agency law enforcement and regulatory endeavor created to target IPR crimes.

As part of this effort, rights holders, online marketplaces, payment processers and companies involved in all points across the supply chain regularly meet with members of the IPR Center to share their best practices, concerns, and suggestions. The information gathered at these events can lead to further collaboration across sectors to develop innovative solutions to complex cross-cutting challenges, including enhanced information sharing, joint enforcement actions, and specialized, targeted training and outreach.

IPR Training

The IPR Center, with assistance from the Department of State, works closely with International Narcotics and Law Enforcement Affairs (DOS/INL) and DOJ International Computer Hacking and Intellectual Property Section (formerly Intellectual Property Law Enforcement Coordinator - IPLEC). In conjunction with ICE Attaché offices, the IPR Center directs, organizes and delivers regional IPR training in the form of lectures and presentations to foreign customs, police, prosecutors, and magistrates.

IPR Center training programs are usually 3-5 days in length and emphasize IPR enforcement, particularly the investigation and prosecution of IPR violations and associated crimes such as smuggling and money laundering.

The training programs are interactive workshops led by subject matter experts and focus on health and safety risks associated with counterfeited items such as pharmaceuticals, electronics, automotive parts, and health and beauty products. With the growing number of e-commerce marketplaces, the training programs have an Internet-investigations focus as well.

Private sector representatives or associations are also invited to participate in the training programs to highlight the challenges their industry sector may face in a particular region and to highlight the necessity of government and industry cooperation.

Automotive Anti-Counterfeiting Council

The IPR Center meets regularly with automotive original equipment manufacturers through the Automotive Anti-Counterfeiting Council (A2C2) to address the sale and distribution of counterfeit parts and components to unsuspecting consumers, including the distribution of counterfeit parts through third-party marketplaces. The IPR Center and the A2C2 work together to provide training to federal and local law enforcement partners and payment processors on recognizing counterfeit automotive parts and conducting criminal investigations and prosecutions.

Defense Industrial Base Supply Chain

Addressing counterfeits in the defense industrial base supply chain is critical to national security. A faulty counterfeit product can harm not only the individual who uses it. It can impact the safety and security of the entire country if dangerous counterfeits are used in combat situations.

The Defense Federal Acquisition Regulation Supplement (DFARS) is a Department of Defense (DOD)-specific supplement to the Federal Acquisitions Regulation (FAR), which establishes government-wide regulations governing executive agency procurement contracts. DFARS 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, requires that certain government contractors institute and implement a counterfeit detection and avoidance system for electronic parts, including establishing the minimum requirements for such a system and penalties for a failure to comply. In addition, contractors can recover the costs of any rework or corrective action taken to remedy any counterfeits parts from subcontractors.

Operation Chain Reaction (OCR) is an ICE-led initiative at the IPR Center that targets counterfeits entering the supply chains of the DOD and other USG agencies. OCR began in June 2011, and it combines the expertise of 17 federal agencies. Each year, the OCR Task Force co-hosts the Counterfeit Microelectronics Working Group (CMWG) with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS). Attendees include representatives from industry, law enforcement, Department of Defense (DOD), and Assistant United States Attorneys (AUSAs). The focus of the meetings is to enhance communication between law enforcement and industry and discuss the latest trends in the counterfeiting of integrated circuits. The CMWG's role is to protect the DOD supply chain through extensive collaboration.

11. Appendix B: Ongoing CBP Activities to Combat Counterfeit Trafficking

This appendix provides a brief summary of some of the major activities CBP and DHS engage in as part of the battle against the trafficking of counterfeit and pirated goods.

National Targeting Center

CBP's National Targeting Center (NTC) carries out daily targeting on IPR recidivists, which often use third-party marketplaces for counterfeit trafficking. It makes referrals to the IPR Center for review and distribution to its field offices for further investigation. It also provides real time IPR case support for Homeland Security Investigations and collaborates with the NTC's investigations division to collaborate on IPR criminal leads and existing cases.

COAC E-Commerce Working Group

The Commercial Customs Operations Advisory Committee (COAC) provides recommendations to the Secretaries of the Treasury and DHS on improvements to the commercial operations of CBP. The COAC consists of 20 members appointed by the Secretary of the Treasury and the Secretary of DHS.

COAC members are representative of the individuals and firms affected by the commercial operations of CBP. CBP's Office of Trade leads the COAC E-Commerce Working Group, which focuses on policy challenges surrounding the increase of e-commerce shipment volumes. The group recently finalized a supply chain map that the COAC recommended CBP use for outreach and policy-making endeavors.

Outreach

Section 311 of the Trade Facilitation and Trade Enforcement Act (TFTEA) (codified at 19 U.S.C. § 4350) calls for DHS to develop and execute an educational awareness campaign aimed at informing international travelers about the legal, economic, and public health and safety impacts of importing IPR-infringing merchandise. There have been four phases to date in the "Truth Behind Counterfeits" IPR public awareness campaign—summer 2017, holidays 2017, summer 2018, and holidays 2018.

During each of these four phases, advertisements have run on large-scale billboards in major U.S. airports throughout the country. There has also been a digital component to the campaign where the ads run on relevant travel-related websites.

CBP continues to partner with the private sector to conduct IPR risk assessments by allowing IPR owners to assist CBP in identifying authentic and low-risk shipments. CBP is also highly engaged with the private sector through participation in the IPR Working Group of the COAC's Trade Enforcement and Revenue Collection Subcommittee, and the Department of Commerce's Industry Trade Advisory Committee on Intellectual Property Rights.

In FY 2018, CBP conducted roundtables to bring together personnel from the law enforcement community and industry stakeholders for information sharing among members. This provided an opportunity for industry stakeholders to share specific industry standards with field personnel working to protect stakeholder rights at the border. In FY 2018, CBP held roundtables at the Automotive and Aerospace Center of Excellence and Expertise IPR Conference.

CBP personnel from headquarters, the ports, the centers, NTC, and the targeting groups also meet regularly with private sector stakeholders and trade associations to discuss trends, technologies, and ways to cooperate on IPR enforcement. CBP maintains IPR enforcement personnel across the country, allowing CBP personnel to meet with businesses and trade associations either at headquarters or in locations close to where the companies are located or do business. CBP personnel regularly meet with brand protection and other corporate officials on a company-specific basis.

Additionally, CBP pursues bilateral and multilateral engagements with foreign counterparts to conduct joint customs IPR enforcement operations, share effective enforcement practices, and exchange information on IPR violations to improve targeting and interdiction of counterfeit and pirated goods.

CBP, in coordination with ICE/HSI, focuses its bilateral engagement efforts on those countries with which CBP and ICE/HSI have a Customs Mutual Assistance Agreement (CMAA) and continues to pursue establishing new CMAAs with foreign governments around the world. CBP attachés stationed at embassies around the world facilitate cooperation through operational planning, information exchange, and sharing best practices between CBP and foreign customs authorities.

Training

CBP's IPR-related training focuses on training front-line and Center of Excellence and Expertise (Center) personnel on how detect, examine, and enforce IPR violations. Several offices within CBP collaborate to provide a robust IPR instructor-led training course that covers IPR seizure authority, enforcement best practices, administrative IPR procedures, and other critical legal and policy topics.

CBP's Office of Trade also conducts IPR webinars to educate port and Center personnel on IPR infringing products. Rights holders provide information on how to recognize IPR-infringing products, labels, and packaging. CBP is also developing a formalized Advanced IPR Enforcement Training course that will expand on the existing IPR Instructor-led Training course to increase students' knowledge of advanced IPR enforcement areas.

Private sector engagement also continues to comprise a significant part of CBP training for frontline personnel. Rights holders are routinely invited to address CBP audiences at local ports and the Centers. CBP also hosts national webinars with rights holders designed to train personnel across the country. Rights holders also provide CBP personnel with product identification guides

that describe methods to distinguish between genuine and infringing products. These guides afford frontline personnel the ability to compare imported merchandise with pictures of genuine products.

Additionally, CBP Regulations and Rulings provide training on advanced detection of trademark/copyright infringement to Import Specialists of the Automotive and Aerospace Center, the Consumer Products and Mass Merchandising Center, and the Apparel, Footwear and Textile Center, as well as to CBP officers at the ports of Newark, New Jersey, and John F. Kennedy Airport.

Rulemakings and Procedures

CBP has recently published two notices of proposed rulemaking related to the protection of intellectual property rights. In the first, CBP proposes to standardize the process by which customs brokers verify the identity of their clients, typically importers. The proposed regulations would formalize the verification process and require that a re-verification process be carried out by brokers every year. This improved broker knowledge is designed to allow for better commercial fraud prevention and revenue protection, and to help prevent the use of shell or shelf companies by importers who attempt to evade the customs laws of the United States. Preventing the use of shell or shelf companies by importers would help reduce the misclassification of merchandise to avoid duties, protect against IPR violations, reduce antidumping/countervailing duty infractions, and reduce the importation of unsafe merchandise.

The second proposal would create a procedure for the disclosure of information otherwise protected by the Trade Secrets Act to a trademark owner when merchandise has been voluntarily abandoned if CBP suspects that the successful importation of the merchandise would have violated U.S. trade laws prohibiting the importation of merchandise bearing counterfeit marks. This regulation will provide greater transparency for partner government agencies, as well as for rights holders; allowing both to reassess and amend their own enforcement strategies in light of contemporaneous attempts to import counterfeit and pirated goods.

Trade Special Operations

A CBP Trade Special Operation (TSO) is a comprehensive and focused trade targeting action conducted during a limited timeframe to address a specific trade enforcement risk, usually in support of one of CBP's Priority Trade Issues (PTIs), which include IPR violations. These operations target high-risk shipments at seaports, airports, CBP's international mail facilities, and express consignment carrier hubs across the United States.

Three related developments have contributed to the growth in the number of national and local TSOs and improved visibility into their results: (1) The implementation of the Automated Targeting System (ATS) Import Targeting module and the updated ATS Import Cargo module at the beginning of FY 2019; (2) the issuance of an updated TSO Standard Operating Procedures in FY 2019; and (3) the ongoing efforts of proactive trade enforcement managers collaborating within CBP's Integrated Trade Targeting Network, which meets monthly and represents all of CBP trade components (Field Offices, Centers, Headquarters, and other offices).

12. Appendix C: Homeland Security Investigations

Homeland Security Investigations (HSI) within DHS's Immigration and Customs Enforcement agency is the principal investigative arm of DHS. It is a vital U.S. asset in combating criminal organizations illegally exploiting America's travel, trade, financial and immigration systems and including the theft of intellectual property.

Investigations

HSI investigates sophisticated, complex conspiracies that span international boundaries. These investigations result in the prosecution of members of transnational criminal organizations and the seizure of illicit proceeds and contraband.

Operation In Our Sites

Since 2010, HSI has been conducting Operation In Our Sites (IOS). This operation targets criminal organizations that distribute dangerous and illicit goods via websites, online platforms, and social media sites.

Initially formed as a U.S.-based initiative for the seizure of domain name registrations, IOS has evolved to develop long term investigations that identify targets and assets in the U.S. and disrupt the financial schemes used by these organizations, both domestically and internationally.

Operation IOS has been expanded to include efforts by various European countries and coordinated by Europol (the European Union's law enforcement agency). These efforts include civil takedowns by private sector companies/groups.

In 2018, 26 countries and dozens of private sector companies participated in IOS, resulted in the criminal seizure of over 33,000 domain name registrations and the civil seizure of over 1.2 million domain name registrations.

In addition, over 2.2 million URL links to e-commerce platforms and social media platforms have been seized as a result of IOS. When a domain name registration is seized as part of IOS, Internet traffic to that site is redirected towards a seizure banner notifying visitors that the site has been seized for offering counterfeits. Since IOS began, there have been more than 177 million views of the IOS seizure banner.

On February 14, 2018, HSI also published its E-Commerce Strategic Plan. It leverages collaboration among private industry, law enforcement, and advocates for a cooperative enforcement approach to identify and dismantle organizations and prosecute people that traffic in dangerous and illicit goods utilizing various e-commerce outlets. These outlets include both the open-net and the dark web along with sales platforms, social media, and a variety of payment processors and shipping methods.

National Cyber-Forensics and Training Alliance

HSI has two staff members at the National Cyber-Forensics and Training Alliance (NCFTA), a non-government organization in Pittsburgh, PA. The professionals at NCFTA work with industry and law enforcement to de-conflict leads and coordinate operations between agencies, as well as to share intelligence and develop investigative referrals. The NCFTA brings together experienced law enforcement agents and analysts, governmental experts, and industry leaders to form an integral alliance between academia, law enforcement, and industry.

E-Commerce Working Group

In November 2017, HSI established the E-Commerce Working Group; it includes representatives from various online marketplaces, payment platforms, and express consignment businesses along with CBP and the FBI. This working group also includes the International Anti-Counterfeiting Coalition, a Washington, D.C.-based non-profit organization devoted to combating product counterfeiting and piracy.

The E-Commerce Working Group meets regularly to facilitate the exchange of intelligence, share best practices, and identify cross-sector collaboration among its members. In late 2018, HSI led a pilot project which involved the sharing of data among the participating online platforms. This pilot project demonstrated that criminal organizations are exploiting multiple online platforms to sell counterfeit items.

HSI is also working with members of the E-Commerce Working Group as they strive to establish, by late 2019, a practice of sustained and timely sharing of large amounts of information between the platforms. Once this has been accomplished, the initiative will be expanded to include participation by the payment platforms and express consignment sectors.

Training

HSI offers an advanced commercial fraud training course entitled “Intellectual Property and Trade Enforcement Investigations.” This two-week training covers a range of intellectual property and trade enforcement topics. Representatives from the consumer electronics, tobacco, automotive, and other industries subject to high counterfeit risk deliver presentations as part of this training. Four sessions of this course were delivered to 120 HSI and CBP attendees in FY 2019.

13. Appendix D: U.S. Government Efforts

Across the interagency, the USG engages in a comprehensive approach to monitor, deter, and prevent the importation, distribution, and sale of counterfeit and pirated goods into the United States. Law enforcement and regulatory agencies, as well as prosecutors and civil complainants all play a role in addressing this issue, especially as it affects the health and safety, economy and national security of the United States. Some aspects of this approach are mode-neutral while others are specific to the international sale of counterfeit and pirated goods through third-party platforms.

This appendix provides a brief summary of some of the major activities of select agencies and entities to address counterfeits and pirated goods sold on third-party marketplaces. This appendix does not present a comprehensive overview of all efforts to address intellectual property violations.

Department of State

The U.S. Department of State has found that increased diplomatic engagement on intellectual property protections at the highest practical levels, supported by interagency engagement and sustained and targeted capacity building, is an effective way to build up the necessary political will to adequately protect IPR overseas. This diplomatic and capacity-building engagement provides evidence of the weight that the U.S. gives to IPR protection worldwide. High-level engagement on IPR also allows U.S. officials the opportunity to educate foreign officials on the economic, social, and cultural benefits of protecting IPR while at the same time warning of the dangers to their economies, public health, and human safety presented by counterfeits and piracy.

The Department of State, through its Bureau of International Narcotics and Law Enforcement Affairs (INL), in consultation with the Bureau of Economic and Business Affairs Office of Intellectual Property Enforcement, supports the U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN).

The GLEN consists of the worldwide deployment of experienced U.S. law enforcement experts to deliver training and technical assistance to foreign law enforcement partners designed to advance operational success. INL also provides assistance to United States Patent and Trademark Office (USPTO) and the DHS IPR Center to enable them to deliver complementary capacity building.

Department of Commerce

The Department of Commerce International Trade Administration's Office of Standards and Intellectual Property OSIP (OSIP) provides domestic outreach events to promote IPR protection in online marketplaces and to educate small and medium sized enterprises on the value of protecting and enforcing their intellectual property rights both domestically and internationally.

Commerce's "STOPfakes Road Shows" represent a unique, interagency outreach event. They are presented in multiple U.S. cities with IPR-intensive industries and provide an array of panel speakers and IPR experts. These Roadshows deliver critically important information about intellectual property to audiences that need it most – start-ups, entrepreneurs, small and medium-sized businesses, independent creators, and inventors.

In addition, OSIP continues to expand the program's unique interactive features. These include guided assistance by CBP officials to assist with trademark recordation and guidance from U.S. Copyright Office officials in registering copyright protections.

USPTO provides policy and technical advice to the Administration and Congress on legislation and other matters relating to civil, criminal, and border enforcement of intellectual property. It is constantly working to improve domestic intellectual property laws and regulations and also seeks to increase public awareness through education on the risks of infringement and the benefits of IPR protection and enforcement.

In 2019, USPTO launched a multi-year, nationwide public awareness campaign with the National Crime Prevention Council in a joint effort to educate U.S. consumers about the dangers of counterfeit goods.

USPTO, including through its Global Intellectual Property Academy (GIPA), provides and participates in technical assistance and capacity-building programs for foreign governments seeking to develop or improve their intellectual property laws and regulations, and to enhance the expertise of those responsible for intellectual property rights enforcement.

Federal Bureau of Investigation

In October 2015, the Federal Bureau of Investigation (FBI) developed a new strategy to combat IPR crime by helping different industry sectors identify common challenges and work together to solve these challenges. The FBI's strategy focuses on building partnerships with key intermediaries in the supply chain for counterfeit and pirated goods, such as e-commerce platforms, payment processors, and the ecosystem for online advertising.

The FBI's strategy also focuses on identifying and pursuing investigations against "systemic enablers" or entities which knowingly facilitate the large-scale infringement of intellectual property rights. As one example of this in action, in 2017 the FBI helped several e-commerce companies re-evaluate their policies regarding the sale of potentially hazardous counterfeit goods online.

At the IPR Center, the FBI helps provide funding and logistical support for the HSI-managed "report IP theft" button, a web-based application for consumers and rights holders to submit complaints to law enforcement regarding suspected infringing activities. The FBI is currently working on developing new analytic tools to help process consumer and rights holder complaints.

U.S. Trade Representative

The Office of the U.S. Trade Representative (USTR) is responsible for developing and coordinating international trade policy for the U.S. government with respect to IPR protections. USTR also oversees negotiations with trading partners, including on IPR issues.

USTR uses a wide range of bilateral and multilateral trade tools to promote strong intellectual property laws and effective enforcement worldwide, reflecting the importance of intellectual property and innovation to the growth of the U.S. economy.

U.S. Food and Drug Administration

The U.S. Food and Drug Administration (FDA) protects the public health by ensuring the safety, efficacy, and security of food, drugs, medical devices, cosmetics and many public health products. One key method that FDA uses to strengthen its public health mission is through regulations and investigations of counterfeit products.

The FDA also issues safety alerts and recalls of dangerous products. The Consumer Product Safety Commission (CPSC) promotes the safety of consumer products by addressing unreasonable risks of injury and developing uniform safety standards. Not surprisingly, counterfeit and pirated products typically do not comply with CPSC requirements.

Consumer Product Safety Commission

CPSC promotes the safety of consumer products by addressing unreasonable risks of injury and developing uniform safety standards. Not surprisingly, counterfeit and pirated products typically do not comply with CPSC requirements.

U.S. Postal Service

As discussed in this report, one critical mission of USPS is to receive advance electronic data (AED) for inbound international mail, originating in 191 different countries. At present, USPS receives AED data from a majority of the inbound international mail it receives. However, it is also required, under the Synthetics Trafficking and Overdose Protection (STOP) Act of 2018, Pub. L. No. 115-271, §§ 8001-8009, 132 Stat. 3893, Title VIII, Subtitle A, to receive AED on all international mail packages by December 31, 2020.

Importantly, USPS provides the its advance electronic data it receives to CBP. This information sharing assists CBP in better targeting packages before the items arrive at the international service centers.

14. Appendix E: Global Initiatives

The proliferation of counterfeit goods on third-party marketplaces is a global problem. This Appendix offers a brief survey of some of the global options and cooperative efforts available to combat the trafficking of counterfeit and pirated goods.

International Organizations

The World Trade Organization's (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights contains disciplines to protect intellectual property that are enforceable through the WTO's Dispute Settlement Body. The World Intellectual Property Organization, a United Nations specialized agency, is a global forum for intellectual property services, policy, information, and collaboration. The World Customs Organization (WCO) leads international customs cooperation, including with respect to the enforcement of intellectual property rights.

The International Police Organization (INTERPOL), in a partnership with Underwriters Laboratories (UL) operates the International IPR Crime Investigators College (IIPCIC). The mission of IIPCIC is to educate global law enforcement and stakeholder groups to effectively combat transnational IPR crime. Over 160 countries have visited the IIPCIC site since its launch and representatives from over 800 law enforcement agencies have enrolled in the training. INTERPOL enables its members to share and access data on crime and criminals, including counterfeit goods.

Europe

Several European government agencies have developed Memoranda of Understandings (MOUs) with the private sector to address counterfeit issues. For example, the European Commission has facilitated an MOU on the sale of counterfeit goods via the internet with major internet platforms and rights holders who are affected by online sales of counterfeit goods. The platforms commit to notice and take down procedures and to taking pro-active and preventive measures, such as the use of monitoring tools allowing detection of illegal content.

The European Commission also concluded an MOU on Online Advertising and IPR in 2018 that extends to trademarks and copyright. Signatories commit to minimize the placement of advertising on websites and mobile applications that infringe on IPR or disseminate counterfeit goods so as to reduce the revenues of these trafficking websites and apps.

In France, through the French Ministry of Economy, postal operators have signed a charter to address counterfeits with rights holders that focuses on outreach, collaboration and training. In December 2018, brand owners and certain online platforms also signed a charter to fight counterfeits online, which organizes cooperation between brand owners, online platforms, and law enforcement authorities and helps implement preventive measures as well as notice and takedown procedures.

There have also been European efforts to enhance technology associated with protecting intellectual property rights. The European Union Intellectual Property Office (EUIPO) held the

inaugural EU Blockathon competition to develop IPR-protection solutions based on blockchain technologies.

The Intellectual Property Crime Coordinated Coalition (IPC3) at Europol provides operational and technical support to law-enforcement agencies and other partners in the EU. The IPC3 has supported more than 50 high-priority cases of intellectual property infringement. It takes down websites used to sell counterfeit merchandise and shut downs illegal operations that use bitcoin.

The City of London Police (CoLP), and IPR Center partner agency, host the Police Intellectual Property Crime Unit (PIPCU). CoLP is funded by the UK Intellectual Property Office to fight criminals who infringe trademark and copyrights. It works with law enforcement agencies in the UK and across the world to arrest criminals who engage in the production, importation and sale of counterfeit goods.

Postal and customs agencies in France and Italy have organized joint operations where all parcels entering the international office of exchanges from targeted countries are screened for counterfeit goods.

Canada

Canada has created Project Chargeback to fight counterfeiting, fraud, and IPR theft by enabling deceived consumers to get their money back. The initiative, which began in 2012, is administered by the Canadian Anti-Fraud Center (CAFC).

Under the authority of Project Chargeback, defrauded consumers can file a complaint with their bank or the CAFC and provide information on the purchase. The CAFC then works with rights holders to confirm that the goods were counterfeit and relays this information to the cardholder's bank.

The cardholder's bank then initiates a charge back against the seller's merchant account. That results in the termination of the merchant's account used by the counterfeiter, and the victims are instructed not to return the counterfeit goods to the seller.

15. References

Following the mandates set forth in President Trump's April 3, 2019, *Memorandum on Combating Trafficking in Counterfeit and Pirated Goods*, the report shall, as its primary goals:

- Analyze available data and other information to develop a deeper understanding of the extent to which online third-party marketplaces and other third-party intermediaries are used to facilitate the importation and sale of counterfeit and pirated goods;
- Identify the factors that contribute to trafficking in counterfeit and pirated goods; and describe any market incentives and distortions that may contribute to third-party intermediaries facilitating trafficking in counterfeit and pirated goods.
- Identify appropriate administrative, statutory, regulatory, or other changes, including enhanced enforcement actions, that could substantially reduce trafficking in counterfeit and pirated goods or promote more effective law enforcement regarding trafficking in such goods.

In the course of pursuing these goals, the report shall also:

- Evaluate the existing policies and procedures of third-party intermediaries relating to trafficking in counterfeit and pirated goods, and identify the practices of those entities that have been most effective in curbing the importation and sale of counterfeit and pirated goods, including those conveyed through online third-party marketplace
- Identify appropriate guidance that agencies may provide to third-party intermediaries to help them prevent the importation and sale of counterfeit and pirated goods.
- Identify appropriate administrative, regulatory, legislative, or policy changes that would enable agencies, as appropriate, to more effectively share information regarding counterfeit and pirated goods, including suspected counterfeit and pirated goods, with intellectual property rights holders, consumers, and third-party intermediaries.
- Evaluate the current and future resource needs of agencies and make appropriate recommendations for more effective detection, interdiction, investigation, and prosecution regarding trafficking in counterfeit and pirated goods, including trafficking through online third-party marketplaces and other third-party intermediaries; and recommend changes to the data collection practices of agencies, including specification of categories of data that should be collected and appropriate standardization practices for data.
- Identify areas for collaboration between the Department of Justice and Department of Homeland Security on efforts to combat trafficking in counterfeit and pirated goods.

See full memorandum at, President Donald J. Trump, Memorandum on Combating Trafficking in Counterfeit and Pirated Goods, 3 April 2019. https://www.whitehouse.gov/presidential-actions/memorandum-combating-trafficking-counterfeit-pirated-goods/